Norbert Klingen

Algebra I

Übungen zur Vorlesung
(mit Lösungen)

Aufgabenstellungen: M. Hofmeister

Universität zu Köln WS 1984/85

Inhaltsverzeichnis

Algebra I

Übung 1

Aufgabe 1. (m)
Welche Gruppen sind Ihnen aus Analysis und Linearer Algebra bereits geläufig? Man entscheide für jede solche Gruppe, ob sie kommutativ ist oder nicht.

Lösung:
Zahlbereiche additiv: $(\mathbb{Z},+) \subset (\mathbb{Q},+) \subset (\mathbb{R},+) \subset (\mathbb{C},+)$ und
multiplikativ $(\{-1,+1\},\cdot) \subset (\mathbb{Q}\setminus\{0\},\cdot) \subset (\mathbb{R}\setminus\{0\},\cdot) \subset (\mathbb{C}\setminus\{0\},\cdot)$, alle kommutativ.
Symmetrische Gruppe $(S_n,\circ)$, nicht kommutativ für $n \geq 3$,
Matrixgruppen $\mathrm{SL}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{C})$, nicht kommutativ für $n \geq 2$.

Aufgabe 2. (m)

a) Bestimmen Sie mögliche Gruppentafeln für Gruppen der Ordnung ≤ 6.

b) Vergleichen Sie die gefundenen Gruppentafeln der Ordnung 4. Gibt es auffällige Gemeinsamkeiten oder Gegensätze?

c) Für jede natürliche Zahl $n \in \mathbb{N}_+$ gebe man die Gruppentafel einer Gruppe der Ordnung n an.

Lösung:
Wir wollen hier – über die Intention der mündlich zu bearbeitenden Aufgabe hinaus – *systematisch alle* möglichen Gruppentafeln bis zur Ordnung 6 aufstellen, und dies weitgehend allein auf der Basis der Gruppendefinition. Der Nachweis, dass die gefundenen Tafeln auch tatsächlich *Gruppen*tafeln sind, also die Assoziativität erfüllt ist, ist hier nicht gefordert. Dieser Nachweis erfolgt auch am besten durch die Angabe bekannter Gruppen (siehe Aufgabe 1) mit den gefundenen Tafeln.
a/b) Wir gehen im folgenden jeweils von einer Gruppe G der gewünschten Ordnung aus und versuchen die Gruppentafel zu bestimmen. Es bezeichne immer e das neutrale Element von G. Gemäß Prop. I.1.3 kommen in den Spalten und Zeilen einer Gruppentafel jeweils *alle* Element *genau einmal* vor.
Für die Gruppen der Ordnung $n \leq 3$ kommt daher jeweils nur eine Tafel in Frage:
$n=1$: $G=\{e\}$.
$n=2$: $G=\{e,a\} \implies a^2=e$.
$n=3$: $G=\{e,a,b\} \implies ab=e=ba$, denn $ab=a \ \vee \ ab=b \implies b=e \ \vee \ a=e$, Wid.
Also ergibt sich nur folgende Tafel:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$n=4$: Sei $G=\{e,a,b,c\}$.
Eines der drei Elemente a,b,c muss sein eigenes Inverses sein, da man 3 Elemente nicht in disjunkte Paare $x \neq x^{-1}$ aufteilen kann. Sei also o. E. $a^2=e$. Dann folgt $ab=c\,, ac=b\,,\ ba=c\,,\ ca=b$. Dies ergibt die nachfolgend angegebene unvollständige Gruppentafel.
Für den Rest ergeben sich die zwei Möglichkeiten: $b^2=c^2 \in \{e,a\}$
1. $b^2=c^2=e \implies bc=cb=a$: Tafel 1.

2. $b^2 = c^2 = a \implies bc = cb = e$: Tafel 2.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c		
c	c	b		

1.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

2.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

ad b): Beide möglichen Gruppen sind kommutativ, in Tafel 1. sind alle Elemente ihre eigenen Inversen und das Produkt von je zwei der drei Elemente $a, b, c \neq e$ ergibt das jeweilige dritte. In Tafel 2. gibt es nur ein selbstinverses Element (a), während die beiden anderen (b, c) zueinander invers sind. Die beiden Tafeln sind grundsätzlich verschieden.

ad a) $\underline{n = 5}$: Sei $G = \{e, a, b, c, d\}$. Wieder betrachten wir die möglichen Inversen.

1. $a^2 = e \implies \left|\begin{array}{ccccc} e & a & b & c & d \\ a & e & & & \end{array}\right. \implies ab \in \{c, d\} \underset{o.E.}{\implies} ab = c \implies ac = a^2b = b \implies ad = d$, Wid.

2. $a^2 \neq e$: $\implies a^2 \in \{b, c, d\} \underset{\text{o.E.}}{\implies} a^2 = b \implies ab \in \{e, c, d\}$.

2.1. $ab = e$: $\implies \left|\begin{array}{ccccc} e & a & b & c & d \\ a & b & e & & \end{array}\right. \implies \begin{cases} ac = d\,, \\ ad = c \end{cases} \implies bc = a^2c = ad = c \implies b = e\,.$ Wid.

2.2. $ab \neq e \implies ab \in \{c, d\} \underset{\text{o.E.}}{\implies} c := ab \implies \left|\begin{array}{ccccc} e & a & b & c & d \\ a & b & c & & \end{array}\right. \implies ac = d\,,\ ad = e\,.$

Damit ist $G = \{e, a, b = a^2, c = a^3, d = a^4\}$ und $e = ad = a^5$. Die Gruppentafel ist die in c) angegebene Tafel (für den Spezialfall $n = 5$).

$\underline{n = 6}$: Sei $G = \{e, v, w, x, y, z\}$. Wieder betrachten wir die Inversen der 5 nicht-trivialen Elemente in G. Es kann maximal zwei Paare von Inversen geben, die anderen Elemente sind selbstinvers.

1. Nur ein Selbstinverses, zwei Paare von Inversen: $vw = xy = e$, $z^2 = e$

Wegen $z \notin \{v, vw = e, vz\} \implies z \in \{v^2, vx, vy\}$.

1.1 $z = v^2$: $\implies \begin{cases} wz = wv^2 = v \implies w = vz \\ w^2 = z^{-1} = z \end{cases} \implies \left|\begin{array}{cccccc} e & v & w & x & y & z \\ v & z & e & & & w \\ w & e & z & & & v \end{array}\right. \implies vx = y = wx$, Wid.

Dies zeigt, dass das selbstinverse Element z kein Quadrat sein kann.

1.2 $z \in \{vx, vy\}$: o. E. $z = vx \implies \begin{cases} wz = x \implies xz = w \\ zy = v \implies zv = y \end{cases}$

$$\implies \left|\begin{array}{cccccc} e & v & w & x & y & z \\ v & & e & z & & \\ w & e & & & & x \\ x & & & & e & w \\ y & & e & & & \\ z & y & & & v & e \end{array}\right. \implies \begin{cases} vz = y \implies z = wy\,, \\ yz = v \implies z = xv\,, \end{cases} \implies \left|\begin{array}{cccccc} e & v & w & x & y & z \\ v & & e & z & & y \\ w & e & & & z & x \\ x & z & & & e & w \\ y & & e & & & v \\ z & y & & & v & e \end{array}\right. \implies v^2 \in \{w, x\}$$

1.2.1 $v^2 = x \implies w^2 = y \implies$

	e	v	w	x	y	z
e	e	v	w	x	y	z
v	v	x	e	z	w	y
w	w	e	y	v	z	x
x	x	z	v	y	e	w
y	y	w	z	e	x	v
z	z	y	x	w	v	e

1.2.2 $v^2 = w \implies w^2 = v \implies$

	e	v	w	x	y	z
e	e	v	w	x	y	z
v	v	w	e	z	x	y
w	w	e	v	y	z	x
x	x	z	y	v	e	w
y	y	x	z	e	w	v
z	z	y	x	w	v	e

Beide Tafeln sind kommutativ, ja, sie sind auch nicht wesentlich verschieden: Im Falle 1.2.1 $v^2 = x$ ergab sich $x^2 = y = x^{-1}$, während im Falle 1.2.2 $v^2 = w = v^{-1}$ umgekehrt $x^2 = v$ ergab. Die 2. Tafel entsteht aus der ersten, indem man die Paare (v, w) und (x, y) austauscht.

2. Drei Selbstinverse, ein Paar von Inversen: $vw = wv$, $x^2 = y^2 = z^2 = e$

2.1 $v^2 \in \{x, y, z\} \underset{\text{o.E.}}{\implies} v^2 = x \implies \begin{cases} w^2 = v^{-2} = x^{-1} = x\,, \\ wx = wv^2 = v \implies vx = wx^2 = w \end{cases}$

$\Longrightarrow$ $\left|\begin{array}{cccccc} e & v & w & x & y & z \\ v & x & e & w & & \\ w & e & x & v & & \end{array}\right.$ $\Longrightarrow$ $\begin{cases} vy = z\,, \\ wy = z \end{cases}$ cr Wid.

2.2 $v^2 = w$: $\Longrightarrow$ $vx \in \{y, z\} \underset{\text{o.E.}}{\Longrightarrow} vx = y \Longrightarrow \left|\begin{array}{cccccc} e & v & w & x & y & z \\ v & w & e & y & & \end{array}\right. \Longrightarrow \begin{cases} vy = z\,, \\ vz = x\,, \end{cases}$ (1)

$\Longrightarrow \begin{cases} wz = wvy = y\,, \\ wx = wvz = z\,, \end{cases} \Longrightarrow \left|\begin{array}{cccccc} e & v & w & x & y & z \\ v & w & e & y & z & x \\ w & e & & z & x & y \end{array}\right. \Longrightarrow w^2 = v\,.$

(1) $\Longrightarrow \begin{cases} xz = vz^2 = v \Longrightarrow xv = x^2z = z \\ zy = vy^2 = v \Longrightarrow zv = z^2y = y \end{cases} \Longrightarrow \left|\begin{array}{cccccc} e & v & w & x & y & z \\ v & w & e & y & z & x \\ w & e & v & z & x & y \\ x & z & & e & & v \\ y & & & & e & \\ z & y & & & v & e \end{array}\right. \Longrightarrow \left|\begin{array}{cccccc} e & v & w & x & y & z \\ v & w & e & y & z & x \\ w & e & v & z & x & y \\ x & z & y & e & w & v \\ y & x & z & v & e & w \\ z & y & x & w & v & e \end{array}\right.$

Unsere Überlegungen zeigen, es gibt höchstens eine Gruppe der Ordnung 6, die drei selbstinverse Elemente enthält, und diese ist nicht kommutativ. Dadurch kann man sie als Tafel einer Ihnen bekannten Gruppe identifizieren (siehe Aufgabe 1) und damit nachweisen, dass es tatsächlich eine *Gruppen*tafel ist und die Verknüpfung assoziativ ist. Alle anderen Gruppenaxiome sind gemäß Prop. I.1.3erfüllt.

3. Alle Elemente selbstinvers: $v^2 = e \Longrightarrow vw \in \{x, y, z\}$, also o. E. $x := vw$

$\Longrightarrow \begin{cases} vx = v^2w = w \Longrightarrow v = wx\,, \\ x = x^{-1} = w^{-1}v^{-1} = wv \end{cases} \Longrightarrow \left|\begin{array}{cccccc} e & v & w & x & y & z \\ v & e & x & w & & \\ w & x & e & v & & \end{array}\right. \Longrightarrow \begin{cases} vy = z\,, \\ wy = z\,, \end{cases}$ Wid.

ad c): Sei $n \in \mathbb{N}_+$, dann erfüllt folgende (additive) Tafel die Forderungen von Prop. I.1.3. Es handelt sich um eine Gruppentafel (die Assoziativität ließe sich in diesem Fall zur Not nachrechnen, aber angesichts der Identifizierung dieser Gruppen als Faktorgruppen von $\mathbb{Z}$ im weiteren Verlauf der Vorlesung nicht sinnvoll.)

$+$	0	1	2	$\ldots$	$n-2$	$n-1$
0	0	1	2	$\ldots$	$n-2$	$n-1$
1	1	2	3	$\ldots$	$n-1$	0
2	2	3	4	$\ldots$	0	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$n-3$	$n-3$	$n-2$	$n-1$	$\ldots$	$n-4$	$n-3$
$n-2$	$n-2$	$n-1$	0	$\ldots$	$n-3$	$n-2$
$n-1$	$n-1$	0	1	$\ldots$	$n-2$	$n-1$

Aufgabe 3. (m)

a) Wiederholen Sie aus der linearen Algebra die geometrische Bedeutung der Elemente in

$$\begin{aligned} \mathrm{O}_2(\mathbb{R}) &= \{A \in \mathrm{GL}_2(\mathbb{R}) \mid A^{-1} = A^{\mathrm{t}}\} \quad \text{und} \\ \mathrm{SO}_2(\mathbb{R}) &= \{A \in \mathrm{O}_2(\mathbb{R}) \mid \det A = 1\}, \end{aligned}$$

wenn man diese als Endomorphismen des $\mathbb{R}^2$ auffaßt.

b) Dem Einheitskreis $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2\}$ sei ein regelmäßiges n-Eck $\mathcal{E}_n$ ($n \geq 3$) mit den Eckpunkten $P_0, \ldots, P_{n-1}$ einbeschrieben, so dass $P_0 = (1, 0)$ ein Eckpunkt ist. Bestimmen Sie alle Eckpunkte P_i.

c) Wieviele Abbildungen f gibt es in $\mathrm{O}_2(\mathbb{R})$ bzw. $\mathrm{SO}_2(\mathbb{R})$ mit $f(\mathcal{E}_n) = \mathcal{E}_n$?

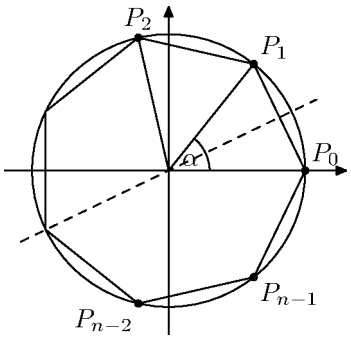
Lösung:

a) $\mathrm{O}_2(\mathbb{R})$ sind die *orthogonalen* Abbildungen der reellen Ebene, die Automorphismen der euklidischen Ebene $\mathbb{R}^2$ mit dem Standardskalarprodukt. Sie haben Determinante ± 1, sie sind *winkel-* und *längentreu*. In der Ebene sind dies die Spiegelungen und Drehungen. Die Elemente

der *speziellen orthogonalen* Gruppe $\mathrm{SO}_2(\mathbb{R})$ sind zusätzlich *orientierungstreu* und daher nur die Drehungen der Ebene.

b) Die Ecken eines regelmäßigen n-Ecks bilden mit dem Mittelpunkt im Koordinatenursprung gleichschenklige Dreiecke mit der Kantenlänge 1. Benachbarte Ecken bestimmen so ein gleichschenkliges Dreieck, dessen Winkel an der Spitze $\alpha = \frac{2\pi}{n}$ beträgt. Also sind die n gesuchten Ecken des regelmäßigen n-Ecks die Punkte

$$P_k = (\cos(k\alpha), \sin(k\alpha)) \in \mathbb{R}^2 \ (k = 0, \ldots, n-1)\,.$$



c) Die Drehung um Vielfache des Winkels α (mit Zentrum im Ursprung) führen das regelmäßige n-Eck in sich über. Dies sind n Abbildungen aus $\mathrm{SO}_2(\mathbb{R})$. Hinzu kommen in $\mathrm{O}_2(\mathbb{R})$ die Spiegelungen an einer Symmetrieachse des regelmäßigen n-Ecks. Die Geraden durch den Ursprung und einen Eckpunkt sind solche Symmetrieachsen, wie etwa die x-Achse. Bei *ungeradem* n sind diese alle verschieden. Bei *geradem* n fallen je zwei davon zusammen, so dass es nur $n/2$ solcher Achsen durch die n Eckpunkte gibt. Aber bei *geradem* n gibt es zusätzlich weitere $n/2$ Symmetrieachsen, nämlich die Winkelhalbierenden der Zentridreiecke benachbarter Punkte (siehe gestrichelte Linie in der Skizze), die bei *geradem* n *nicht* durch einen gegenüberliegenden Eckpunkt verlaufen (eigene Skizze!). Die Gesamtzahl der Spiegelungen ist also in jedem Falle n. Fazit:

$$\#\{f \in \mathrm{SO}_2(\mathbb{R}) \mid f(\mathcal{E}_n) = \mathcal{E}_n\} = n\,, \qquad \#\{f \in \mathrm{O}_2(\mathbb{R}) \mid f(\mathcal{E}_n) = \mathcal{E}_n\} = 2n\,.$$

Aufgabe 4. (m)
Sei A eine Menge und G die Menge aller Bijektionen von A auf A. Zeigen Sie, dass G mit der Komposition von Abbildungen eine Gruppe ist. Unter welchen Bedingungen an A kann man die Forderung der Bijektivität abschwächen?

Lösung:
Für Selbstabbildungen $f, g : A \to A$ ist die Komposition $f \circ g$ und $g \circ f$ stets definiert und assoziativ. $\mathrm{id}_A \in G$ ist neutrales Element bzgl. $\circ$. Ist $f \in G$, so existiert zu jedem $b \in A$ ein $a \in A$ mit $f(a) = b$ (Surjektivität) und a ist eindeutig zu b bestimmt (Injektivität). Daher wird durch $\check{f}(b) := a$ eine Abbildung $\check{f} : A \to A$ definiert und es gilt $f \circ \check{f} = \check{f} \circ f = \mathrm{id}_A$. Daher ist $\check{f} \in G$ Inverses zu $f \in G$ und G eine Gruppe.
Nur wenn A einelementig ist, kann auf die Forderung der Bijektivität verzichtet werden (sie ist trivialerweise erfüllt). Für *endliches* A genügt allein die Forderung der In- oder der Surjektivität, denn:

$$f : A \to A \text{ injektiv } \implies \#(f(A)) = \#A \implies f(A) = A\,.$$

und für surjektives, aber nicht-injektives $f : A \to A$ folgt bei endlichem A der Widerspruch

$$\bigvee_{a \neq b} f(a) = f(b) \implies f(A \setminus \{a\}) = f(A) = A \implies \#(A \setminus \{a\}) \geq \#A, \text{ Wid.}$$

Aufgabe 5. (m)
Es gibt wichtige binäre Verknüpfungen, die *nicht* zu einer Gruppenstruktur führen. Wir betrachten dazu die Menge $C^\infty(\mathbb{R})$ der beliebig oft differenzierbaren Funktionen $f : \mathbb{R} \to \mathbb{R}$. Auf dieser definieren wir die binäre Verknüpfung $[.,.]$ vermöge der sog. *Lieklammer* $[f, g] = f'g - fg'$. Sind die folgenden Aussagen richtig oder falsch?

a) $C^\infty(\mathbb{R})$ besitzt ein neutrales Element bzgl. $[.,.]$.

b) Die Lieklammer ist assoziativ.

c) $[[f, g], h] + [[g, h], f] + [[h, f], g] = 0$ für alle $f, g, h \in C^\infty(\mathbb{R})$.

Lösung:
a) Falsch: Wäre e neutral, also $f = f'e - fe'$ für alle f, so folgte:

$$\bigwedge_{x\in\mathbb{R}} f(x) = 1 \implies 1 = -e'(x) \iff \bigvee_{c\in\mathbb{R}} e(x) = -x + c\,,$$
$$\bigwedge_{x\in\mathbb{R}} f(x) = x \implies x = e(x) - xe'(x) = -x + c + x = c \in \mathbb{R},\ \text{Wid.}$$

b) Falsch: $[f,1] = f' \implies [[f,1],1] = f''$, $[f,[1,1]] = [f,0] = 0$, also für $f(x) = x^2$ keine Gleichheit.
c) Richtig:

$$\begin{aligned}
[[f,g],h] &= (f'g - fg')'h - (f'g - fg')h' \\
&= (f''g + f'g' - f'g' - fg'')h - (f'g - fg')h' \\
&= f''gh - fg''h - f'gh' + fg'h' \\
[[f,g],h] + [[g,h],f] + [[h,f],g] &= (f''gh - fg''h - f'gh' + fg'h') \\
&\quad +(g''hf - gh''f - g'hf' + gh'f') \\
&\quad +(h''fg - hf''g - h'fg' + hf'g') \\
&= 0
\end{aligned}$$

Aufgabe 6. (m)
Geben Sie Beispiele an für Gruppen G mit Untergruppen U, die folgende Bedingungen erfüllen:

a)	$\#G = \infty$,	$(G:U) = \infty$,	$\#U = \infty$
b)	$\#G = \infty$,	$(G:U) = \infty$,	$1 < \#U < \infty$
c)	$\#G = \infty$,	$1 < (G:U) < \infty$,	$\#U = \infty$
d)	$\#G < \infty$,	$1 < (G:U)$,	$1 < \#U$

Lösung:
a) $G = (\mathbb{Q}, +)$, $U = \mathbb{Z}$, $(G:U) = \infty$, denn $x + \mathbb{Z} \neq y + \mathbb{Z}$ für alle $0 \leq x, y < 1$, $x \neq y$.
b) $G = (\mathbb{Q} \setminus \{0\}, \cdot)$, $U = \{\pm 1\}$
c) $G = (\mathbb{Z}, +)$, $U = 2\mathbb{Z}$, $(G:U) = 2$, denn $G = 2\mathbb{Z} \,\dot\cup\, (1 + 2\mathbb{Z})$.
c) $G = S_3$ symmetrische Gruppe, $U = A_3$ alternierende Gruppe.

Algebra I

Übung 2

Aufgabe 7. (m)

a) Sei G eine Gruppe und $H \subseteq G$ eine nicht-leere Teilmenge. Zeigen Sie:

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

b) Ist $(\mathbb{Z}, +)$ die Gruppe der ganzen Zahlen, so ist für alle $m \in \mathbb{Z}$ $H := m\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$.

Lösung:
a) $\Rightarrow$ ist klar, da die Untergruppe H gegenüber den Gruppenoperationen Multiplikation und Inversenbildung abgeschlossen ist.
ad $\Leftarrow$: H besitzt 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 gemäß Bemerkung I.1.7.
b) Wir wenden a) an auf die additive abelsche Gruppe $(\mathbb{Z}, +)$: $0 \in m\mathbb{Z}$ und $a = mx, b = my \in m\mathbb{Z} \implies a - b = m(x - y) \in m\mathbb{Z}$, so dass b) aus a) folgt.

Aufgabe 8. (m)
Sei $i \in \mathbb{C}$ die imaginäre Einheit und seien

$$E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in M_2(\mathbb{C})\,.$$

Zeigen Sie, dass die Menge $Q_8 := \{\pm E, \pm I, \pm J, \pm K\}$ bzgl. der Matrixmultiplikation eine nicht-abelsche Gruppe der Ordnung 8 ist, die sog. *Quaternionengruppe.*

Lösung:
Wir berechnen (1): $I^2 = J^2 = K^2 = -E$, also sind alle Matrizen aus Q_8 invertierbar und die Inversen von I, J, K sind das jeweilige Negative. Q_8 liegt also in der *Gruppe* $\mathrm{GL}_2(\mathbb{C})$ und ist gegen Inversenbildung abgeschlossen.
Q_8 ist auch multiplikativ abgeschlossen: Dazu berechnen wir die Produkte
(2): $IJ = K\,,\ JK = I\,,\ KI = J$: Das Produkt von zweien ergibt die dritte Matrix bei richtiger, zyklisch fortgesetzter Reihenfolge I, J, K. Mit der 'Inversenformel' (1) erhalten wir daraus, dass bei Umkehrung der Faktoren I, J, K sich das Negative ergibt (alles natürlich auch leicht direkt nachzurechnen):

$$-K = K^{-1} = (IJ)^{-1} = J^{-1}I^{-1} = (-J)(-I) = JI\,, \quad KJ = -I\,, \quad IK = -J\,.$$

Damit ist die Multiplikationstafel von Q_8 vollständig: Q_8 ist auch multiplikativ abgeschlossen und daher eine Untergruppe von $\mathrm{GL}_2(\mathbb{C})$; sie ist nicht abelsch.

Aufgabe 9. (s)

a) Sei G eine zyklische Gruppe von gerader Ordnung $2n$. Zeigen Sie, dass es in G genau ein Element der Ordnung 2 gibt.

b) Sei G zyklisch von der Ordnung m. Zeigen Sie: Das Produkt aller Elemente von G ist e, falls m ungerade ist, und gleich dem (gemäß a)) einzigen Element der Ordnung 2, wenn m gerade ist.

c) Zeigen Sie: Die nicht-trivialen Gruppen G ohne echte Untergruppen sind genau die von Primzahlordnung; diese sind zyklisch.

Lösung:
a) Sei $G = \langle a \rangle$, also $\operatorname{ord} a = \#G = 2n$. Dann gilt für $a^k \in G$ $(0 \le k < 2n)$

$$\operatorname{ord} a^k = 2 \iff a^k \neq e \ \wedge \ a^{2k} = e \iff 2n \mid 2k \neq 0 \iff n \mid k \neq 0 \iff n = k\,.$$

b) G ist abelsch, also ist das Produkt $A = \prod\limits_{x \in G} x$ aller Elemente von der Reihenfolge unabhängig und daher wohldefiniert.

$$A^2 = \prod_{x \in G} x \cdot \prod_{x \in G} x^{-1} = \prod_{x \in G} (x x^{-1}) = e\,.$$

Also ist $A = e$ oder $\operatorname{ord} A = 2$. Ist $\operatorname{ord} A = 2$, so ist 2 ein Teiler von $\#G = m$. Bei ungeradem m muss also $A = e$ sein.
Sei nun m gerade und z das nach a) eindeutig bestimmte Element der Ordnung 2. Dann gilt: $x \neq e, z \implies x^2 \neq e \iff x \neq x^{-1}$ und wir können A wie folgt darstellen:

$$A = e \cdot z \cdot \prod_{x \neq x^{-1}} x = z$$

denn in dem letzten Produkt kommt mit jedem x auch sein Inverses $x^{-1} \neq x$ vor, das Produkt ist e.
c) Sei $\#G = p$ eine Primzahl und $H \le G$ 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 $e \neq a \in G$: $\langle a \rangle = G$, G ist zyklisch.
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 10. (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 $\exp(G) = \operatorname{kgV}\{\operatorname{ord}(g) \mid g \in G\}$.

b) Jede Gruppe vom Exponenten 2 ist abelsch.

c) Für zyklisches G gilt $\exp(G) = \#G$.

Lösung:
a) Wegen der Endlichkeit von G gilt $g^{\#G} = e$ (Satz von Lagrange, Vorlesung I.1.13, S. 8), also haben alle $g \in G$ endliche Ordnung $\operatorname{ord} g$ und es gilt $\exp(G) \le \#G < \infty$. Mit $\exp := \exp(G)$ und $\operatorname{kgV} := \operatorname{kgV}(\operatorname{ord}(g) \mid g \in G)$ gilt gemäß Prop. 1.10 d) (S. 6)

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

und umgekehrt

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

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 $\exp(G) \le \#G$ und für zyklisches $G = \langle a \rangle$ gilt nach a) $\#G = \operatorname{ord}(a) \mid \exp(G)$.

Aufgabe 11. (s)
Wir definieren auf dem $\mathbb{R}^2$ die folgende Verknüpfung: $(x_1, x_2) * (y_1, y_2) = (x_1 + y_1 e^{x_2}, x_2 + y_2)$.

a) Zeigen Sie, dass $G = (\mathbb{R}^2, *)$ eine Gruppe und $H = \{0\} \times \mathbb{R}$ eine Untergrupe darin ist.

b) Bestimmen Sie die Rechts- und Linksnebenklasse von $(a, 0)$ bzgl. H.

c) Stellen Sie für $a \in \{0, \pm 1\}$ die Nebenklassen $H * (a, 0)$, $(a, 0) * H$ graphisch dar.

Lösung:
a) Die Verknüpfung ist assoziativ:

$$(x_1 + y_1 e^{x_2}, x_2 + y_2) * (z_1, z_2) = (x_1 + y_1 e^{x_2} + Z_1 e^{x_2+y_2}, x_2 + y_2 + z_2),$$
$$(x_1, x_2) * (y_1 + z_1 e^{y_2}, y_2 + z_2) = (x_1 + (y_1 + z_1 e^{y_2}) e^{x_2}, x_2 + y_2 + z_2).$$

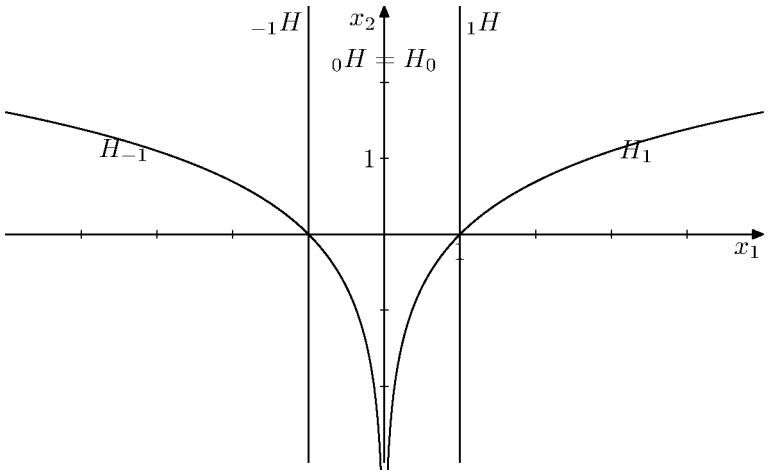
$(0, 0)$ ist neutrales Element: $(x_1, x_2) * (0, 0) = (x_1, x_2)$, $(0, 0) * (y_1, y_2) = (0 + y_1 e^0, y_2) = (y_1, y_2)$.

$$(0, 0) = (x_1 + y_1 e^{x_2}, x_2 + y_2) \iff y_2 = -x_2 \wedge 0 = x_1 + y_1 e^{x_2} \iff y_2 = -x_2 \wedge y_1 = -x_1 e^{-x_2},$$

also ist $(-x_1 e^{-x_2}, -x_2)$ Linksinverses von (x_1, x_2) bzgl. $*$. Es ist auch Rechtsinverses:

$$(x_1, x_2) * (-x_1 e^{-x_2}, -x_2) = (x_1 - x_1 e^{-x_2} e^{x_2}, 0) = (0, 0).$$

H ist Untergruppe, denn $(0, x_2) * (0, y_2) = (0, x_2 + y_2)$.
b) Wir berechnen $(a, 0) * (0, x_2) = (a, x_2)$, also $(a, 0) * H = \{(a, x_2) \mid x_2 \in \mathbb{R}\}$: Die Linksnebenklassen ${}_aH = (a, 0) * H$ von H sind die Parallelen zur x_2-Achse.
$(0, x_2) * (a, 0) = (0 + e^{x_2} a, x_2)$, also $H * (a, 0) = \{(ae^{x_2}, x_2) \mid x_2 \in \mathbb{R}\}$: Die Rechtsnebenklassen $H_a = H * (a, 0)$ sind die Graphen der Funktionen $g_a(x_2) = ae_2^x$ (mit x_2 als Funktionsvariable).



Aufgabe 12. (s)
Es sei $M_n(\mathbb{Z})$ die Menge aller $n \times n$-Matrizen mit ganzzahligen Koeffizienten und $\mathrm{GL}_n(\mathbb{Q})$ die allgemeine lineare Gruppe über $\mathbb{Q}$. Zeigen Sie:

a) $M_n(\mathbb{Z}) \cap \mathrm{GL}_n(\mathbb{Q})$ ist bzgl. der Matrixmultiplikation keine Gruppe.

b) Die Teilmenge $\mathrm{GL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}$ ist eine Gruppe, die Gruppe der n-reihigen *unimodularen* Matrizen. Sie ist die größte Untergruppe von $\mathrm{GL}_n(\mathbb{Q})$, die in $M_n(\mathbb{Z})$ enthalten ist.

c) Geben Sie für jedes $n \in \mathbb{N}$ ein $A \in \mathrm{GL}_n(\mathbb{Z})$ an, das als Einträge nicht nur 0 und ± 1 enthält.

Lösung:
a) $A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \in M_2(\mathbb{Z})$ hat Determinante 2 und als Inverses

$$A^{-1} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \notin M_n(\mathbb{Z})\,.$$

Wir erweitern Matrizen aus $M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})$ zu n-reihigen Matrizen, indem man sie mit Einsen auf der Hauptdiagonale und sonst Nullen auffüllt. Die dadurch entstehende erweiterte Matrix $\hat{A} \in M_n(\mathbb{Z})$ hat als Inverses die Erweiterung $\widehat{A^{-1}} \notin M_n(\mathbb{Z})$.
b) Entsprechend der Determinantendefinition hat jede ganzzahlige Matrix auch ein ganzzahlige Determinante: $A \in M_n(\mathbb{Z}) \implies \det A \in \mathbb{Z}$. Ist also $H \leq \mathrm{GL}_n(\mathbb{Q})$ eine Untergruppe mit $H \subseteq M_n(\mathbb{Z})$, so gilt

$$A, A^{-1} \in H \subset M_n(\mathbb{Z}) \implies \det A, \frac{1}{\det A} \in \mathbb{Z} \implies \det A = \pm 1\,,$$

also liegt $H \subset \mathrm{GL}_n(\mathbb{Z})$. Damit bleibt zu zeigen, dass $\mathrm{GL}_n(\mathbb{Z})$ eine Untergruppe von $\mathrm{GL}_n(\mathbb{Q})$ ist. $\mathrm{GL}_n(\mathbb{Z})$ enthält die Einheitsmatrix und ist multiplikativ abgeschlossen. Schließlich folgt mit Hilfe der bekannten Inversenformel aus der Linearen Algebra

$$A \in \mathrm{GL}_n(\mathbb{Z}) \implies A^{-1} = \frac{1}{\det A} A^{\mathrm{ad}} = \pm A^{\mathrm{ad}} \in M_n(\mathbb{Z})\,,$$

wobei A^{ad} die Adjunkte von A ist. Deren Einträge sind Determinanten von Teilmatrizen von A und daher ganzzahlig. Damit ist $\mathrm{GL}_n(\mathbb{Z})$ auch gegenüber Inversenbildung abgeschlossen und also eine Untergruppe.
c) Für $n = 2$ wähle man etwa $\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ oder $\begin{pmatrix} 5 & 2 \\ 3 & 1 \end{pmatrix}$ und für $n \geq 3$ erweitere man diese Matrizen wie in a) erläutert zu Matrizen in $\mathrm{GL}_n(\mathbb{Z})$.

Algebra I

Übung 3

Aufgabe 13. (s)

a) Eine Gruppe $G = \{e, a, b, c\}$ der Ordnung 4 heißt *Kleinsche Vierergruppe,* wenn gilt $a^2 = b^2 = c^2 = e$ (e das Einselement von G). Wieviele Kleinsche Vierergruppen gibt es?

b) Eine Kleinsche Vierergruppe ist Vereinigung von drei echten Untergruppen. Kann eine Gruppe Vereinigung von *zwei* echten Untergruppen sein?

c) Zeigen Sie, dass in beliebigen Gruppen Untergruppen vom Index 2 Normalteiler sind.

Lösung:
a) Die geforderten Eigenschaften legen die Gruppentafel eindeutig fest: Jedes Gruppenelement ist sein eigenes Inverses. Daher muss $ab \neq e$ sein und wegen $a \neq e \neq b$ ist $ab \neq a, b$ und es kommt nur $ab = c$ in Frage. Genauso argumentiert man für alle anderen Produkte: Das Produkt von je zwei verschiedenen der Elemente a, b, c ergibt das dritte. Es gibt höchstens eine Kleinsche Vierergruppe. (Siehe auch Aufgabe 2, Fall $n = 4$, Fall 1.) Andererseits überprüft man leicht, dass

$$\mathcal{V}_4 := \{\mathrm{id}, (1\,2)(3\,4)\,,\ (1\,3)(2\,4)\,,\ (1\,4)(2\,3)\} \subset S_4$$

eine Kleinsche Vierergruppe im oben definierten Sinne ist.
b) Wegen $a^2 = e$ ist $\langle a\rangle = \{e, a\}$ Untergruppe von $\mathcal{V}_4$, genauso $\{e, b\}$ und $\{e, c\}$. Ihre Vereinigung ist ganz $\mathcal{V}_4$.
Sei nun G eine beliebige Gruppe, Vereinigung von zwei echten Untergruppen U, V: $G = U \cup V$. Dann gibt es $a, b \in G$ mit $a \notin U$, also $a \in V$ und umgekehrt $b \notin V, b \in U$. Deren Produkt ab liegt in $G = U \cup V$, also in U oder V, aber $ab \in U \ \wedge\ b \in U \implies a \in U$, Wid. also $ab \in V$, aber das ist genauso unmöglich. Mit zwei echten Untergruppen kann man eine Gruppe *nicht* überdecken.
c) Sei $U \leq G$ und $(G : U) = 2$. Dann gilt für jedes $a \in G \setminus U$: $G = U \,\dot\cup\, Ua$ und $G = U \,\dot\cup\, aU$ und damit $Ua = G \setminus U = aU$, also $aUa^{-1} = U$ für alle $a \notin U$. Für $a \in U$ gilt natürlich $aUa^{-1} = U$, womit U als Normalteiler nachgewiesen ist.

Aufgabe 14. (m)
Es sei G eine Gruppe. Zeigen Sie: Ist $G/\mathrm{Zentr}(G)$ zyklisch, so ist G abelsch.

Lösung:
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 $a, b \in G$.

Aufgabe 15. (s)
Sei G eine Gruppe mit Untergruppen $H_1, H_2 \leq G$. 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 ist.

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

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 $b_i H_1$ 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 $\bigwedge_{g \in G} \bigvee_{i \in I}\ g \in gH_1 = b_i H_1 \subset H_2 H_1 \implies G = H_2 H_1$.
Die H_i sind als Untergruppen von G gegen Inversenbildung abgeschlossen, also gilt auch $G = G^{-1} = (H_2 H_1)^{-1} = H_1^{-1} H_2^{-1} = H_1 H_2$.
Umgekehrt: Ist $G = H_2 H_1$, 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 16. (s)
Für $n \in \mathbb{N}_+$ definieren wir die Gruppe $D_{2n} \leq \mathrm{O}_2(\mathbb{R})$ durch

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

Zeigen Sie:

a) $\operatorname{ord} S = 2$, $\operatorname{ord} R_n = n$ und $R_n \cdot S = S \cdot R_n^{-1}$. D_{2n} ist eine Gruppe der Ordnung $2n$.

b) Für $n \geq 3$ ist D_{2n} die Symmetriegruppe des regelmäßigen n-Ecks $\mathcal{E}_n$, d. h. die Gruppe der orthogonalen Abbildungen $f \in \mathrm{O}_2(\mathbb{R})$, die $\mathcal{E}_n$ auf sich abbilden (vgl. Aufgabe 3). Sie wird *Diedergruppe* der Ordnung $2n$ genannt[1)].

c) D_2 ist zyklisch, D_4 Kleinsche Vierergruppe und $D_6 \simeq S_3$ und D_{2n} ist nicht abelsch für $n \geq 3$.

Lösung:
a) Wiederholende Übungen zur Matrixrechnung aus der Linearen Algebra. Es ist $S^2 = E$, $R_n^l = \begin{pmatrix} \cos\frac{2l\pi}{n} & -\sin\frac{2l\pi}{n} \\ \sin\frac{2l\pi}{n} & \cos\frac{2l\pi}{n} \end{pmatrix}$ und $R_n S = S R_n^{-1}$. Wegen $R_n^l = E \iff \frac{2l\pi}{n} \in 2\pi\mathbb{Z} \iff n \mid l\,,$ ist $\operatorname{ord} R_n = n$. Damit enthält D_{2n} die zyklische Untergruppe $\langle R_n \rangle$ mit der Ordnung n. Deren Index ist 2, denn $\det S = -1 \implies S \notin \langle R_n \rangle$, und damit gilt $\#D_{2n} = 2 \cdot n$..
b) Die geometrische Bedeutung der Erzeugenden als Endomorphismen des $\mathbb{R}^2$ ist klar: S ist die Spiegelung an der x-Achse und R_n ist die Drehung um den Winkel $\frac{2\pi}{n}$. Beide gehören also zur Symmetriegruppe des n-Ecks, und damit liegt auch die erzeugte Gruppe D_{2n} darin. Nach a) und Aufgabe 3 haben beide Gruppen gleiche Ordnung, stimmen also überein.
c) $n = 1 \implies R_1 = E \implies D_2 = \{E, S\}$ mit $S^2 = E$ Einheitsmatrix.
$n = 2 \implies \operatorname{ord} S = \operatorname{ord} R_2 = 2 \underset{a)}{\implies} SR_2 = R_2 S \implies D_4 = \{E, S, R_2, SR_2\}$ und $\operatorname{ord}(SR_2) = 2$.
Die drei Elemente $\neq E$ haben die Ordnung 2 und damit ist D_4 die Kleinsche Vierergruppe (siehe Aufgabe 13 a)).
$n \geq 3 \implies \operatorname{ord} R_n = n > 2 \implies R_n^{-1} \neq R_n \underset{\text{a)}}{\implies} SR_n \neq R_n S$, also ist D_{2n} nicht-abelsch.

[1)] Die Bezeichnungen sind hier nicht immer einheitlich: Statt D_{2n} wird sie wegen ihrer Operation auf dem n-Eck auch als Diedergruppe D_n vom *Grade* n bezeichnet. Man vergewissere sich beim Blick in die Literatur immer über die *Ordnung* der Gruppe.

D_{2n} permutiert die Ecken des regelmäßigen n-Ecks $\mathcal{E}_n$ und liefert so einen Homomorphismus $D_{2n} \to S_n$ in die symmetrische Gruppe vom Grade n. Dieser ist injektiv, da $\mathcal{E}_n$ eine Basis des $\mathbb{R}^2$ enthält. Für $n = 3$ ergibt dies eine Einbettung von D_6 in S_3, die wegen gleicher Mächtigkeit ein Isomorphismus ist.

Aufgabe 17. (s)
Seien G, H Gruppen und $f, g : G \to H$ Gruppenhomomorphismen. Zeigen Sie:

a) Stimmen f und g auf einem Erzeugendensystem von G überein, so gilt $f = g$ auf ganz G.

b) Ist K ein minimales Erzeugendensystem einer Gruppe G der Ordnung n, so gilt $\#K \leq \log_2 n$.

[Tipp: Für ein minimales Erzeugendensystem $K = \{a_1, \ldots, a_r\}$ betrachten Sie die erzeugten Untergruppen $G_k := \langle a_1, \ldots, a_k \rangle$.]

c) Es sei $\mathrm{Aut}(G)$ die Automorphismengruppe von G. Ist G endlich von der Ordnung n und K ein Erzuegendensystem von G, so gibt es höchstens $n^{\#K}$ Automorphismen von G. Folgern Sie: $\#G = n \implies \#(\mathrm{Aut}(G)) \leq n^{\frac{\log n}{\log 2}}$.

Lösung:
a) Sei für alle $a \in K$ $f(a) = g(a)$, also $K \subset H := \{a \in G \mid f(a) = g(a)\}$. Da f, g Endomorphismen sind, ist H eine Untergruppe von G und folglich $H \geq \langle K \rangle = G$: $f = g$ auf ganz G.
b) Sei $K = \{a_1, \ldots, a_r\}$ ein minimales, d. h. nicht verkleinerbares Erzeugendensystem von G. Wegen der Minimalität kan man kein a_k aus dem Erzeugendensystem weglassen, also gilt für alle $k < r$ $a_{k+1} \notin \langle a_1, \ldots, a_k \rangle =: G_k$ und daher $G_k \subsetneq G_{k+1}$. Damit ist $\#G_{k+1} = \#G_k \cdot (G_{k+1} : G_k) \geq 2\#G_k$. Zusammen mit $G_1 \neq \{e\}$, also $\#G_1 \geq 2$ folgt $\#G_k \geq 2^k$ für alle k und damit $n = \#G = \#G_r \geq 2^r$. Dies bedeutet $\#K = r \leq \log_2 n$.
c) Nach b) ist die Restriktionsabbildung $f \mapsto f|_K$ eine *injektive* Abbildung von der Automorphismengruppe in die Menge G^K aller Abbildungen von K in G und daher

$$\#\mathrm{Aut}\, G \leq \#(G^K) = \#G^{\#K} = n^{\#K} \underset{\text{b)}}{\leq} n^{\log_2(n)}\,.$$

Aufgabe 18. (s)
Seien G, G_1, G_2 Gruppen und $f_i : G \twoheadrightarrow G_i$ Gruppenepimorphismen $(i = 1, 2)$. Zeigen Sie:

$$\text{a)} \qquad \mathrm{Ke}\, f_1 \subseteq \mathrm{Ke}\, f_2 \iff \bigvee_{\varphi: G_1 \to G_2 \text{ Hom.}} f_2 = \varphi \circ f_1$$

$$\text{b)} \qquad \mathrm{Ke}\, f_1 = \mathrm{Ke}\, f_2 \iff \bigvee_{\varphi: G_1 \to G_2 \text{ Isom.}} f_2 = \varphi \circ f_1$$

Lösung:
a) $\Leftarrow$ ist klar, denn $a \in \mathrm{Ke}\, f_1 \implies f_2(a) = \varphi(f_1(a)) = \varphi(e) = e \implies a \in \mathrm{Ke}\, f_2$.
$\Rightarrow$: f_1 ist surjektiv, also existiert zu jedem $a_1 \in G_1$ ein $a \in G$ mit $a_1 = f_1(a)$. Wir setzen nun $\varphi(a_1) := f_2(a)$ und zeigen, dass $\varphi : G_1 \to G_2$ wohldefiniert ist:

$$a_1 = f_1(a) = f_1(a') \implies a'a^{-1} \in \mathrm{Ke}\, f_1 \subset \mathrm{Ke}\, f_2 \implies f_2(a) = f_2(a') = \varphi(a_1)\,.$$

Genauso leicht überprüft man, dass φ ein Gruppenhomomorphismus ist:

$$a_1 = f_1(a)\,,\ a_1' = f_1(a') \implies \varphi(a_1 a_1') = f_2(aa') = f_2(a) f_2(a') = \varphi(a_1)\varphi(a_1')\,.$$

Zusatz: Da f_2 surjektiv ist, muss auch φ surjektiv sein.
b) $\Leftarrow$: Nach a) gilt $\mathrm{Ke}\, f_1 \subseteq \mathrm{Ke}\, f_2$. Aus $f_2 = \varphi \circ f_1$ mit einem *Iso*morphismus $\varphi : G_1 \to G_2$ folgt $f_1 = \varphi^{-1} \circ f_2$ und man erhält a) auch die umgekehrte Inklusion $\mathrm{Ke}\, f_2 \subseteq \mathrm{Ke}\, f_1$.
$\Rightarrow$: Nach a) existieren Homomorphismen $\varphi : G_1 \to G_2$, $\psi : G_2 \to G_1$ mit $f_1 = \psi \circ f_2 = \psi \circ \varphi \circ f_1$, also $\psi \circ \varphi = \mathrm{id}_{\mathrm{Im}\, f_1} = \mathrm{id}_{G_1}$. Aufgrund der Symmetrie erhält man genauso $\varphi \circ \psi = \mathrm{id}_{G_2}$, φ und ψ sind (zueinander inverse) Isomorphismen.

Algebra I

Übung 4

Aufgabe 19. (m)
Es sei $f : G \to H$ ein Homomorphismus von Gruppen und $N \lhd \operatorname{Im} f$ ein Normalteiler. Zeigen Sie: $f^{-1}(N) \lhd G$ und $\operatorname{Im} f/N \simeq G/f^{-1}(N)$.

Lösung:
$\bar{f} := \nu_N \circ f : G \twoheadrightarrow \operatorname{Im} f \twoheadrightarrow \operatorname{Im} f/N$ ist ein Epimorphismus mit Kern $\operatorname{Ke} \bar{f} = f^{-1}(N)$ und die Behauptung folgt aus dem Homomorphiesatz I.1.20 a): $G/f^{-1}(N) = G/\operatorname{Ke} \bar{f} \xrightarrow{\sim} \operatorname{Im} \bar{f} = \operatorname{Im} f/N$.

Aufgabe 20. (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:
$\alpha)$ $\tau_k := (k, k+1) \in \langle \sigma_n, \tau \rangle$ für alle $1 \leq k < n$.
$\beta)$ $(i, j) = \tau_{j-1} \circ \ldots \circ \tau_{i+1} \circ \tau_i \circ \tau_{i+1} \ldots \circ \tau_{j-1}$ 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) $\alpha)$ $\tau_k = (k, k+1) = (\sigma_n^{k-1}(1), \sigma_n^{k-1}(2)) \underset{\text{b)}}{=} \sigma_n^{k-1} \circ (1, 2) \circ \sigma_n^{-(k-1)} \in \langle \sigma_n, \tau \rangle$.
$\beta)$ 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) $\beta)$ ist jede Transposition Produkt von Elementen τ_k, die nach c) $\alpha)$ in $\langle \sigma_n, \tau \rangle$ liegen.

Aufgabe 21. (s)

a) Beweisen Sie den Satz von Cayley: Jede Gruppe ist isomorph zu einer Permutationsgruppe.

b) Folgern Sie: Jede endliche Gruppe der Ordnung n ist isomorph zu einer Untergruppe von $\mathrm{GL}_n(\mathbb{Z})$, den n-reihigen unimodularen Matrizen (siehe Aufgabe 12).

[Tipp: Permutationsmatrizen.]

c) Stellen Sie die Quaternionengruppe Q_8 (siehe Aufgabe 8) als Permutationsgruppe und als Untergruppe von $\mathrm{SL}_8(\mathbb{Z}) := \{A \in \mathrm{GL}_8(\mathbb{Z}) \mid \det A = +1\}$ dar.

d) Kann man Q_8 auch als Untergruppe von $\mathrm{SL}_4(\mathbb{Z})$ darstellen?

Lösung:
a) Sei G eine Gruppe. Jedes Element $a \in G$ definiert durch Linksmultiplikation eine Selbstabbildung $L_a : G \to G$ von G durch $L_a(b) = ab$. $L_{a^{-1}}$ ist invers zu L_a, also ist L_a eine bijektive Selbstabbildung von G, also ein Element der symmetrischen Gruppe $\mathcal{S}(G)$ über G. Die dadurch definierte Abbildung

$$L : G \to \mathcal{S}(G)\,,\ a \mapsto L_a$$

ist ein Gruppenmonomorphismus von G in die symmetrische Gruppe $(\mathcal{S}(G), \circ)$:

$$L_{ab}(x) = abx = L_a \circ L_b(x) \quad \text{und} \quad L_a = L_b \implies L_a(e) = L_b(e) \iff a = b\,.$$

b) Sei $B = \{e_1, \ldots, e_n\}$ die kanonische Basis des $\mathbb{R}^n$. Dann induziert jede Permutaion $\sigma \in S_n$ eine Permutation der Basis B ($e_i \mapsto e_{\sigma i}$ entsprechend der vorgegebenen Abzählung) und diese ist eindeutig fortsetzbar zu einem Automorphismus $\varphi_\sigma \in \mathrm{Aut}(\mathbb{R}^n) \simeq \mathrm{GL}_n(\mathbb{R})$. Dessen Matrix bzgl. B ist gegeben durch die sog. Permutationsmatrix

$$P_\sigma = (\delta_{i,\sigma j})_{ij} = \left(\, e_{\sigma 1} \middle| e_{\sigma 2} \middle| \cdots \middle| e_{\sigma(n-1)} \middle| e_{\sigma\, n} \, \right) \quad \text{mit} \quad \det P_\sigma = \operatorname{sign} \sigma\,.$$

Die Permutationsmatrizen sind also unimodular und die Abbildung $P : S_n \to \mathrm{GL}_n(\mathbb{Z})$ ist ein Gruppenmonomorphismus.
c) Wir erinnern an die Multiplikationsformeln (1): $I^2 = J^2 = K^2 = -E$ und (2): $IJ = K\,,\ JK = I\,,\ KI = J$ für Q_8 (siehe Lösung von Aufgabe 8 oder direkt nachrechnen). Damit berechnen wir die Linksmultiplikationen L_I und L_J auf Q_8 als Permutationen von $Q_8 = \{E, -E, I, -I, J, -J, K, -K\}$:

$$L_I = \begin{pmatrix} E & -E & I & -I & J & -J & K & -K \\ I & -I & -E & E & K & -K & -J & J \end{pmatrix} = (E, I, -E, -I) \circ (J, K, -J, -K)\,,$$
$$L_J = \begin{pmatrix} E & -E & I & -I & J & -J & K & -K \\ J & -J & -K & K & -E & E & I & -I \end{pmatrix} = (E, J, -E, -J) \circ (I, -K, -I, K)\,,$$

bzw. bei Nummerierung der Elemente von Q_8 gemäß der obigen Auflistung

$$\sigma_I = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 7 & 8 & 6 & 5 \end{pmatrix} = (1\,3\,2\,4)\,(5\,7\,6\,8)\,,$$
$$\sigma_J = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 8 & 7 & 2 & 1 & 3 & 4 \end{pmatrix} = (1\,5\,2\,6)\,(3\,8\,4\,7)\,,$$

$$Q_8 \xrightarrow{\sim} \langle (1\,3\,2\,4)(5\,7\,6\,8), (1\,5\,2\,6)(3\,8\,4\,7) \rangle \subset \mathcal{A}_8 \subset \mathcal{S}_8$$

Als unimodulare Matrixdarstellung ergibt sich so $Q_8 \xrightarrow{\sim} \langle P_I, P_J \rangle \subset \mathrm{SL}_8(\mathbb{Z})$ mit

$$P_I = \left(\, e_3 | e_4 | e_2 | e_1 | e_7 | e_8 | e_6 | e_5 \, \right) \quad \text{und} \quad P_J = \left(\, e_5 | e_6 | e_8 | e_7 | e_2 | e_1 | e_3 | e_4 \, \right) \in \mathrm{SL}_8(\mathbb{Z})\,.$$

Explizit

$$P_I = \left(\begin{array}{cc|cc|cc|cc} & & 0 & 1 & & & & \\ & & 1 & 0 & & & & \\ \hline 1 & 0 & & & & & & \\ 0 & 1 & & & & & & \\ \hline & & & & & & 0 & 1 \\ & & & & & & 1 & 0 \\ \hline & & & & 1 & 0 & & \\ & & & & 0 & 1 & & \end{array}\right), \quad P_J = \left(\begin{array}{cc|cc|cc|cc} & & & & 0 & 1 & & \\ & & & & 1 & 0 & & \\ \hline & & & & & & 1 & 0 \\ & & & & & & 0 & 1 \\ \hline 1 & 0 & & & & & & \\ 0 & 1 & & & & & & \\ \hline & & 0 & 1 & & & & \\ & & 1 & 0 & & & & \end{array}\right) \in \mathrm{SL}_8(\mathbb{Z})$$

In dieser Darstellung sind zur Verdeutlichung reine 0-Blöcke nicht ausgeschrieben. So wird die Struktur als 4×4-Matrix von 2×2-Matrizen gut sichtbar.

d) Eine Darstellung in $\mathrm{GL}_4(\mathbb{Z})$ ist möglich, wenn man von der ursprünglichen Definition der Matrizen $I, J, K \in \mathrm{GL}_2(\mathbb{C})$ ausgeht. Es ist $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$ und daher ist die Linksmultiplikation mit $0 \neq z = x + iy$ auf $\mathbb{C} \simeq \mathbb{R}^2$ ein $\mathbb{R}$-Automorphismus mit der Matrix $L_z = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$. Speziell $L_{\pm i} = \begin{pmatrix} 0 & \mp 1 \\ \pm 1 & 0 \end{pmatrix}$. Setzt man dies, zusammen mit $L_{\pm 1} = \pm E \in \mathrm{GL}_2(\mathbb{R})$, in die Definitionen von I, J ein, so erhält man aus $I_2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$ die Matrizen

$$I_4 = \begin{pmatrix} L_i & 0 \\ 0 & L_{-i} \end{pmatrix} = \left(\begin{array}{cc|cc} 0 & -1 & 0 & \\ 1 & 0 & & \\ \hline & & 0 & 1 \\ 0 & & -1 & 0 \end{array}\right), \quad J_4 = \left(\begin{array}{cc|cc} & & 1 & 0 \\ 0 & & 0 & 1 \\ \hline -1 & 0 & & \\ 0 & -1 & 0 & \end{array}\right) \in \mathrm{SL}_4(\mathbb{Z}),$$

und damit eine Darstellung $Q_8 \rightsquigarrow \langle I_4, J_4 \rangle \leq \mathrm{SL}_4(\mathbb{Z})$.

Zusatz: Man kann auch die in c) bestimmte Darstellung von Q_8 in $\mathrm{SL}_8(\mathbb{Z})$ durch folgende Überlegung zu einer Darstellung in $\mathrm{SL}_4(\mathbb{Z})$ 'komprimieren'. Die Darstellungsmatrizen $P_I, P_J \in \mathrm{SL}_8(\mathbb{Z})$ sind 4×4-Matrizen, bei denen in jeder Zeile bzw. Spalte nur je einmal entweder die Einheitsmatrix $E_2 \in M_2(\mathbb{Z})$ oder die selbstinverse Matrix $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{Z})$ auftritt. M und E_2 bilden zusammen eine multiplikative Untergruppe in $M_2(\mathbb{Z})$ der Ordnung 2. Allein auf Basis dieser Tatsachen berechnet sich die Isomorphie $\langle P_I, P_J \rangle \simeq Q_8$. Ersetzt man nun E_2 bzw. M durch $+1$ bzw. $-1 \in \mathbb{Z}$, so erhält man aus P_I und P_J die folgenden Matrizen I_4, J_4 mit denselben Relationen wie P_I, P_J und damit wieder eine Darstellung von Q_8:

$$I_4 = \left(\begin{array}{cc|cc} 0 & -1 & & \\ 1 & 0 & & \\ \hline & & 0 & -1 \\ & & 1 & 0 \end{array}\right), \quad J_4 = \left(\begin{array}{cc|cc} & & -1 & 0 \\ & & 0 & 1 \\ \hline 1 & 0 & & \\ 0 & -1 & & \end{array}\right) \in \mathrm{SL}_4(\mathbb{Z})$$

und

$$Q_8 \rightsquigarrow \langle P_I, P_J \rangle \rightsquigarrow \langle I_4, J_4 \rangle \leq \mathrm{SL}_4(\mathbb{Z}).$$

Aufgabe 22. (s)
Sei $n \in \mathbb{N}, n \geq 3$. Wir definieren in der symmetrischen Gruppe $\mathcal{S}_n$ die Elemente

$$\begin{aligned} \sigma_n &:= (1\,2\,\ldots\,n), \\ \tau_n &:= (1, n-1) \circ (2, n-2) \circ \ldots \circ (\lfloor \frac{n-1}{2} \rfloor, n - \lfloor \frac{n-1}{2} \rfloor) \\ &= (1, n-1) \circ (2, n-2) \circ \ldots \circ \begin{cases} (\frac{n-1}{2}, \frac{n+1}{2}) & n \text{ ungerade}, \\ (\frac{n}{2} - 1, \frac{n}{2} + 1) & n \text{ gerade}. \end{cases} \end{aligned}$$

und die Permutationsgruppe $G := \langle \sigma_n, \tau_n \rangle \leq \mathcal{S}_n$. Zeigen Sie:

a) $\operatorname{ord}\sigma_n = n$, $\operatorname{ord}\tau_n = 2$, $\sigma_n\tau_n = \tau_n\sigma_n^{-1}$ und jedes $\rho \in G$ ist eindeutig darstellbar als $\rho = \sigma_n^\mu\tau_n^\nu$ mit $0 \le \mu \le n-1$ und $0 \le \nu \le 1$.

b) G ist isomorph zur Diedergruppe D_{2n} der Ordnung $2n$ (siehe Aufgabe 16).

c) Geben Sie eine geometrische Beschreibung von G.

Lösung:
Siehe auch Vorlesung, Beispiele I.2.14 4).
a) $\operatorname{ord}\sigma_n = n$, da die Ordnung von Zyklen deren Länge ist. $\operatorname{ord}\tau_n = 2$, da elementfremde Zyklen vertauschbar sind und Transpositionen die Ordnung 2 haben. Für die Vertauschbarkeitsformel benutzen wir Aufgabe 20 b):

$$\tau_n^{-1} \circ (1\,2\,\ldots\,n) \circ \tau_n = (\tau_n(1), \tau_n(2), \ldots, \tau_n(n)) = (n-1, n-2, \ldots, 2, 1, n) = \sigma_n^{-1}\,.$$

Elemente von G sind Potenzprodukte von σ_n und τ_n und wegen der Vertauschungsformel kann man die Potenzen von τ_n (vorne oder hinten) sammeln und erhält so für jedes $\rho \in G$ die Darstellung $\rho = \sigma_n^\mu\tau_n^\nu$. Dabei sind $0 \le \mu < \operatorname{ord}\sigma_n = n$ und $0 \le \nu < 2 = \operatorname{ord}\tau_n$ wählbar. Diese Darstellung ist eindeutig, denn für μ, ν im genannten Bereich gilt

$$e = \sigma_n^\mu\tau_n^\nu \iff \tau_n^\nu = \sigma_n^\mu \implies n = \tau_n^\nu(n) = \sigma_n^\mu(n) \implies \mu = 0 \implies \nu = 0\,.$$

b) Seien $S, R_n \in \mathrm{O}_2(\mathbb{R})$ wie in Aufgabe 16 definiert. Wegen der eindeutigen Darstellung aus Aufgabenteil a) hat G die Ordnung $2n$ und die Zuordnung

$$\varphi : G \to D_{2n}\,,\ \sigma_n^\mu\tau_n^\nu \mapsto R_n^\mu S^\nu$$

ist wohldefiniert. Nach a) erfüllen τ_n und σ_n dieselben Relationen wie die Matrizen S und R_n aus Aufgabe 16, so dass die Abbildung $G \to D_{2n}$ ein Homomorphismus ist. Er ist surjektiv, da R_n, S im Bild von φ liegen und D_{2n} erzeugen. Wegen $\#G = 2n = \#D_{2n}$ ist φ ein Isomorphismus.
c) Die hier definierte Permutationsgruppe G ist nichts anderes als die Einschränkung der Diedergruppe $D_{2n} \le O_2(\mathbb{R})$ auf die Ecken $P_1, \ldots, P_n$ des n-Ecks $\mathcal{E}_n$, genauer: Die Spiegelung S an der ersten Achse des $\mathbb{R}^2$ operiert als die Permutation τ_n, die Drehung R_n operiert als zyklus σ_n. Siehe dazu die Skizze in der Lösung von Aufgabe 3 und beachten Sie $P_0 = P_n$. Diese geometrische Deutung liefert zugleich einen anschaulicheren Beweis für b).

Aufgabe 23.
Entfällt

Algebra I

Übung 5

Aufgabe 24. (m)
Zeigen Sie: $\mathrm{Zentr}(\mathrm{GL}_n(\mathbb{R})) = \mathbb{R}^\times \cdot E$, die Gruppe der Skalarmatrizen $\neq 0$.

Lösung:
Sei $A = (a_{ij}) \in \mathrm{Zentr}(\mathrm{GL}_n(\mathbb{R}))$, also $P^{-1}AP = A$ für alle $P \in \mathrm{GL}_n(\mathbb{R})$. Dies bedeutet, das der durch A definierte Automorphismus φ des $\mathbb{R}^n$ bzgl. *jeder* Basis des $\mathbb{R}^n$ *dieselbe* Matrix A hat. Bei einer beliebigen Permutation der Basis werden die Einträge entsprechend permutiert: $a_{ij} = a_{\sigma i,\sigma j}$. Also $a_{ii} =: a$ für alle i und $a_{ij} =: b$ für alle $i \neq j$. Angenommen $b \neq 0$. Dann wechseln wir die Basis von $v_1, \dots v_n$ zu $v_1 + v_2, v_2, \dots v_n$ und es gilt

$$\varphi(v_1+v_2) = av_1 + b(v_2 + \dots v_n) + bv_1 + av_2 + b(v_3 + \dots + v_n) = (a+b)(v_1+v_2) + b(v_3 + \dots + v_n)\,.$$

Wenn sich bei diesem Basiswechsel die Matrix nicht ändern soll, muss $a+b = a$, also $b = 0$ sein. Fazit: $A = aE$ mit $a \in \mathbb{R}$, $a \neq 0$ wengen $\det A \neq 0$.

Aufgabe 25. (m)
Die Gruppe G operiere auf der Menge $\Omega \neq \emptyset$. Zeigen Sie:

a) Für $\alpha \in \Omega$ ist $G_\alpha := \{\sigma \in G \mid \sigma\alpha = \alpha\}$ eine Untergruppe von G, die *Fixgruppe* von α.

b) Es gilt $G_{\sigma\alpha} = \sigma G_\alpha \sigma^{-1}$ für alle $\alpha \in \Omega$ und $\sigma \in G$.

c) Die Länge einer Bahn unter der Operation von G ist ein Gruppenindex; genauer:

$$\#G\alpha = (G : G_\alpha) \quad \text{für alle } \alpha \in \Omega\,.$$

d) Operiert G transitiv auf Ω, so ist $G\alpha = \Omega$ für alle $\alpha \in \Omega$ und $\#\Omega$ Teiler der Gruppenordnung.

Lösung:
a) Es ist $e \in G_\alpha$. für $\sigma, \tau \in G_\alpha$ gilt $\sigma\alpha = \alpha = \tau\alpha$, also auch $\tau^{-1}\alpha = \alpha$ und daher $\sigma\tau^{-1}(\alpha) = \alpha$, $\sigma\tau^{-1} \in G_\alpha$.
b) $\rho \in G_{\sigma\alpha} \iff \sigma\alpha = \rho\sigma\alpha \iff \alpha = \sigma^{-1}\rho\sigma\alpha \iff \sigma^{-1}\rho\sigma \in G_\alpha \iff \rho \in \sigma G_\alpha \sigma^{-1}$.
c) Die Abbildung $G \to G\alpha$, $\sigma \mapsto \sigma\alpha$ ist surjektiv und es gilt

$$\sigma\alpha = \tau\alpha \iff \alpha = \sigma^{-1}\tau\alpha \iff \sigma^{-1}\tau \in G_\alpha \iff \sigma G_\alpha = \tau G_\alpha\,.$$

Also ist die Abbildung $G/G_\alpha \to G\alpha$, $\sigma G_\alpha \mapsto \sigma\alpha$ wohldefiniert und bijektiv, und das bedeutet: $(G : G_\alpha) = \#(G/G_\alpha) = \#G\alpha$.
c) Operiert G transitiv, so existiert bei gegebenem $\alpha \in \Omega$ zu jedem $\beta \in \Omega$ ein $\sigma \in G$ mit $\beta = \sigma\alpha \in G\alpha$, also $\Omega \subset G\alpha \subset \Omega$: Ganz Ω ist eine Bahn. Nach c) ist jede Bahnlänge als Gruppenindex ein Teiler der Gruppenordnung.

Aufgabe 26. (s)
Seien G eine Gruppe, $H \leq G$ eine Untergruppe und $M \subseteq G$ eine Teilmenge. Zeigen Sie für den

$$\textit{Zentralisator} \text{ von } M \text{ in } H \quad \mathrm{Zentr}_H(M) := \{\sigma \in H \mid \bigwedge_{\alpha \in M} \sigma \cdot \alpha = \alpha \cdot \sigma\} :$$

a) $\mathrm{Zentr}_H(M) = \mathrm{Zentr}_H(\langle M \rangle)$ ist eine Untergruppe von H.

b) $N \triangleleft G \implies \mathrm{Zentr}_H(N) \triangleleft G$.

c) $\mathrm{Zentr}_{\mathcal{S}_4}(\mathcal{V}_4) = \mathcal{V}_4$.

Lösung:
a) Es ist $e \in Z$. Für $\sigma, \tau \in Z$ gilt $\sigma\tau\alpha = \sigma\alpha\tau = \alpha\sigma\tau$, also $\sigma\tau \in Z$. Und aus $\sigma\alpha = \alpha\sigma$ folgt nach 'beidseitiger' Multiplikation mit σ^{-1}: $\alpha\sigma^{-1} = \sigma^{-1}\alpha$, also $\sigma^{-1} \in Z$. Damit ist $Z \leq G$.
Genauso zeigt man (mit vertauschten Rollen von σ und α) für $\sigma \in Z$ und $\alpha, \beta \in M$: $\sigma\alpha\beta = \alpha\beta\sigma$ und auch $\sigma\alpha^{-1} = \alpha^{-1}\sigma$ und damit folgt $\sigma \in \mathrm{Zentr}_H(\langle M\rangle)$.
b) Wieder sei $Z := \mathrm{Zentr}_H(N)$ und $\sigma \in Z\,,\ \rho \in G$ beliebig. Dann gilt

$$\bigwedge_{\alpha\in N} \sigma\alpha = \alpha\sigma \implies \bigwedge_{\alpha\in N} \sigma^\rho\alpha^\rho = \alpha^\rho\sigma^\rho \implies \bigwedge_{\beta\in N^\rho = N} \sigma^\rho\beta = \beta\sigma^\rho \implies \sigma^\rho \in Z\,.$$

Damit ist $Z \lhd G$.
c) $\mathcal{V}_4 = \{\mathrm{id}, (1\,2)(3\,4)\,, (1\,3)(2\,4)\,, (1\,4)(2\,3)\}$ besteht neben der Identität aus allen Produkten von 2 elementfremden Transpositionen in $\mathcal{S}_4$. $\mathcal{V}_4$ ist abelsch, also $\mathcal{V}_4 \subset Z := \mathrm{Zentr}_{\mathcal{S}_4}(\mathcal{V}_4)$. Umgekehrt:

$$\sigma \in Z \implies (1\,2)(3\,4) = \sigma(1\,2)(3\,4)\sigma^{-1} \underset{\text{Aufg.20}}{=} (\sigma 1\,, \sigma 2)(\sigma 3\,, \sigma 4) \implies (\sigma 1, \sigma 2) = \begin{cases} (1\,2) \\ (3\,4) \end{cases}$$

Genauso folgt aus der Vertauschbarkeit mit $(1\,3)(2\,4)$ bzw. $(1\,4)(2\,3)$

$$(\sigma 1, \sigma 3) = \begin{cases} (1\,3) \\ (2\,4) \end{cases}, \quad (\sigma 1, \sigma 4) = \begin{cases} (1\,4) \\ (2\,3) \end{cases}.$$

Hat σ einen Fixpunkt, o. E. $\sigma 1 = 1$, so muss jeweils der erste Fall gelten und damit $\sigma i = i$ für alle i, $\sigma = \mathrm{id}$. Ist $\sigma 1 \neq 1$, o. E. $\sigma 1 = 2$, so folgt $\sigma 2 = 1$ und dann (wegen $\sigma 3 \neq 3$) $\sigma = (1\,2)(3\,4)$. In jedem Falle gilt also $\sigma \in Z \implies \sigma \in \mathcal{V}_4$.

Aufgabe 27. (s)
Sei G eine Gruppe und $n \in \mathbb{N}_+$. Zeigen Sie:

a) Genau dann besitzt G eine Untergruppe vom Index n. wenn G transitiv auf einer n-elementigen Menge operiert.

   [Tipp: Aufgabe 25 c) und die Operation auf Nebenklassen.]

b) Besitzt G eine Untergruppe vom Index n, so auch einen echten Normalteiler vom Index $\leq n!$. [Tipp: Gruppenoperationen sind Permutationsdarstellungen.]

c) Echte Untergruppen der alternierenden Gruppe $\mathcal{A}_5$ haben höchstens die Ordnung 12.

Lösung:
a) $\Rightarrow$: Sei $U \leq G$ eine Untergruppe vom Index n, also hat $\Omega = G/U = \{aU \mid a \in G\}$ die Mächtigkeit n. G operiert auf Ω durch Linksmultiplikation

$$\Omega \ni aU \mapsto \sigma aU \quad \text{für } \sigma \in G\,.$$

Diese Operation ist transitiv, denn $aU, bU \in \Omega \implies bU = \sigma aU$ für $\sigma = ba^{-1} \in G$.
$\Leftarrow$: G operiere transitiv auf Ω mit $\#\Omega = n$. Dann ist für ein beliebiges $\alpha \in \Omega$ die Bahn $G\alpha = \Omega$ und die Fixgruppe $U := G_\alpha$ eine Untergruppe von G vom Index $(G : U) = (G : G_\alpha) = \#G\alpha = \#\Omega = n$ (siehe Aufgabe 25).
b) Sei $U \leq G$ eine Untergruppe vom Index n und $G \times \Omega \to \Omega$ die nach a) existierende Operation von G auf einer n-elementigen Mengen Ω. Diese Operation bestimmt einen Gruppenhomomorphismus $L : G \to \mathcal{S}_\Omega$, $\sigma \mapsto L_\sigma$ mit $L_\sigma(\alpha) = \sigma\alpha$. Der Kern $N := \mathrm{Ke}\,L$ dieses Homomorphismus ist ein Normalteiler und dessen Index ist nach dem Homomorphiesatz $(G : \mathrm{Ke}\,L) = \#L(G) \mid \#\mathcal{S}_\Omega = n!$. Wegen $N \leq U$ ist N ein echter Normalteiler in G.
c) Sei $U \leq \mathcal{A}_5$ mit $12 < \#U < 60$. Dann hat U einen Index $1 < n < 5$ und nach b) muss dann $\mathcal{A}_5$ einen echten Normalteiler N vom Index $\leq n! < 60$ enthalten. Dieser wäre dann ein nicht-trivialer Normalteiler von $\mathcal{A}_5$ im Widerspruch zu Satz I.2.7.

Aufgabe 28. (s)
Sei G eine Gruppe und $N \neq \{e\}$ ein Normalteiler in G. Zeigen Sie:

a) G operiert auf $N^* := N \setminus \{e\}$ durch Konjugation und induziert dadurch einen Gruppenhomorphismus $\varphi : G \to \mathcal{S}(N^*)$ von G in die symmetrische Gruppe über N^*.

b) Der Kern von φ ist der Zentralisator $\mathrm{Zentr}_G(N)$ und die Faktorgruppe $G/\mathrm{Zentr}_G(N)$ ist isomorph zu einer Untergruppe der symmetrischen Gruppe $\mathcal{S}(N^*)$.

c) Hat eine Gruppe G einen Normalteiler N der Ordnung 3 und $N \not\subset \mathrm{Zentr}(G)$, so ist 6 ein Teiler von $\#G$.

Lösung:
a) Da N Normalteiler von G ist, operiert G durch Konjugation auf N:

$$a \in N\,,\ \sigma \in G \implies \sigma a \sigma^{-1} \in N\,.$$

Dabei gilt für alle $\sigma \in G$ $\sigma a \sigma^{-1} = e \iff a = e$, also operiert G auf N^*. Diese Operation induziert einen Gruppenhomomorphismus

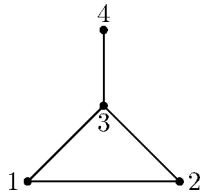
$$\varphi : G \to \mathcal{S}(N^*)\,,\ \sigma \mapsto \iota_\sigma\,|_{N^*} = \sigma(\ldots)\sigma^{-1}\,|_{N^*}\ .$$

b) Es gilt für $\sigma \in G$:

$$\sigma \in \mathrm{Ke}\,\varphi \iff \varphi(\sigma) = \mathrm{id}_{N^*} \iff \bigwedge_{a \in N^*} \sigma a \sigma^{-1} = a \iff \bigwedge_{a \in N} \sigma a = a\sigma \iff \sigma \in \mathrm{Zentr}_G(N)\,.$$

Nach dem Homomorphiesatz gilt also $G/\mathrm{Zentr}_G(N) \xrightarrow{\sim} \mathrm{Im}\,\varphi \leq \mathcal{S}(N^*)$.
c) $N \not\subset \mathrm{Zentr}(G) \iff \mathrm{Zentr}_G(N) \neq G$, also ist nach b) $G/\mathrm{Zentr}_G(N)$ eine nicht-triviale Untergruppe von $\mathcal{S}(N^*) \simeq S_2$. Der Zentralisator $\mathrm{Zentr}_G(N)$ hat also den Index 2 in G und $\#G$ ist gerade. Wegen $3 = \#N \mid \#G$ folgt die Behauptung.

Aufgabe 29. (s)
Ein *Graph* ist ein Paar $(E, \mathcal{K})$ bestehend aus einer endlichen Menge E (den *Ecken)* und einer Menge $\mathcal{K}$ von 2-elementigen Teilmengen von E, den *Kanten.* Zwei Ecken $i \neq j \in E$ eines Graphen sind *benachbart,* wenn $\{i, j\}$ zu $\mathcal{K}$ gehört, also eine Kante ist. Die *Ordnung* (oder *Valenz)* $v(i)$ einer Ecke i ist die Zahl der benachbarten Ecken: $v(i) = \#\{j \in E \mid \{i, j\} \in \mathcal{K}\}$. Graphen werden veranschaulicht durch Punkte (als Ecken) und Verbindungstrecken, die die Kanten symbolisieren.

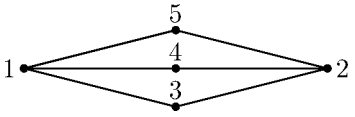


Ein *Automorphismus* eines Graphen ist eine Permutation $\sigma : E \to E$ der Ecken, die Kanten in Kanten überführt: $K \in \mathcal{K} \implies \sigma(K) \in \mathcal{K}$. Zeigen Sie:

a) Die Menge der Automorphismen eines Graphen $(E, \mathcal{K})$ bildet eine Gruppe, die *Automorphismengruppe* $\mathrm{Aut}(E)$ des Graphen.

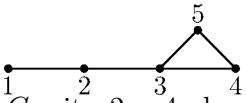
b) Liegen $i, j \in E$ in einer Bahn unter der Operation von $G = \mathrm{Aut}(E)$, so haben sie dieselbe Valenz. Gilt auch die Umkehrung?

c) Bestimmen Sie die Automorphismengruppe des oben skizzierten Graphen. Zeigen Sie, dass die Automorphismengruppe des nachstehend skizzierten Graphen (isomorph zu) $\mathbb{Z}/2\mathbb{Z} \times \mathcal{S}_3$ ist.

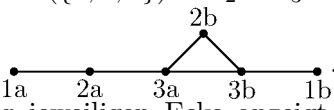


d) Geben Sie einen Graphen mit mindestens zwei Ecken und trivialer Automorphismengruppe an.

Lösung:
a) Man beachte lediglich, dass ein Automorphismus eine injektive Selbstabbildung $\mathcal{K} \ni K = \{i,j\} \mapsto \{\sigma i, \sigma j\} = \sigma(K) \in \mathcal{K}$ der Kantenmenge $\mathcal{K}$ induziert, die wegen der Endlichkeit von $\mathcal{K}$ ebenfalls eine Bijektion ist.
b) Sei $\mathcal{N}(i) := \{j \in E \mid \{i,j\} \in \mathcal{K}\}$ die Menge der Nachbarn von i. Dann gilt für $\sigma \in \mathrm{Aut}(E)$ $\sigma(\mathcal{N}(i)) = \mathcal{N}(\sigma i)$ und damit $v(i) = v(\sigma i)$. Die Ecken in einer Bahn haben also dieselbe Ordnung.

Die Umkehrung gilt nicht: Dazu betrachten wir folgenden Graphen: 

Die Ecken 2 und 4 haben dieselbe Ordnung 2. Angenommen es gibt ein $\sigma \in G$ mit $\sigma 2 = 4$, dann ist $\sigma 1$ benachbart zu $\sigma 2 = 4$, also $\sigma 1 = 3$ oder $\sigma 1 = 5$. Aber $v(1) \neq v(3), v(5)$, Wid. Damit liegen die Ecken 2,4 trotz gleicher Ordnung nicht in einer Bahn unter G.
c) Ein Automorphismus des ersten Graphen der Aufgabenstellung (4 Ecken) muss die Ecken 4 bzw. 3 festlassen, da es keine anderen Ecken mit gleicher Ordnung (1 bzw. 3) gibt. Neben der Identität ist die Transposition $(1\,2)$ der einzig mögliche Automorphismus. Sie bildet die Nachbarn $\mathcal{N}(1) = \{2,3\}$ und $\mathcal{N}(2) = \{1,3\}$ aufeinander ab. Die Automorphismengruppe ist $\langle (1\,2) \rangle$, zyklisch von der Ordnung 2.
Für den zweiten Graphen (5 Ecken) müssen die beiden Ecken $1,2$ der Ordnung 3 und die drei Ecken $3,4,5$ der Ordnung 2 untereinander permutiert werden. Wegen $\mathcal{N}(1) = \mathcal{N}(2) = \{3,4,5\}$ und $\mathcal{N}(3) = \mathcal{N}(4) = \mathcal{N}(5) = \{1,2\}$ können die Ecken 1,2 bzw. 3,4,5 unabhängig voneinander beliebig permutiert werden: $G = \mathcal{S}(\{1,2\}) \times \mathcal{S}(\{3,4,5\}) \simeq \mathcal{S}_2 \times \mathcal{S}_3$.

d) Wir erweitern den Graphen aus b) zu 

. Dabei sind die Ecken so bezeichnet, dass die Zahl die Ordnung der jeweiligen Ecke anzeigt. Sei σ ein beliebiger Automorphismus. Dann gilt $\sigma(1a) \in \{1a, 1b\}$. Wäre $\sigma(1a) = 1b$, so wäre $\sigma(2a) = 3b$, was wegen unterschiedlicher Ordnungen nicht möglich ist. Also $\sigma(1a) = 1a\,,\ \sigma(1b) = 1b.\ \sigma(2a) = 2b$ ist nicht möglich, da $2a$ einen Nachbarn der Ordnung 1 hat, $2b$ jedoch nicht; also $\sigma(2a) = 2a\,,\ \sigma(2b) = 2b$. Genauso folgt $\sigma(3a) \neq 3b$ und damit $\sigma = \mathrm{id}$.

Algebra I
Übung 6

Aufgabe 30. (m)
Entscheiden Sie, welche der folgenden Gruppen zueinander isomorph sind:

1) Diedergruppe D_8 (siehe Aufgabe 16).

2) Quaternionengruppe Q_8 (siehe Aufgabe 8).

3) $\mathbb{Z}/8\mathbb{Z}$ 4) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ 5) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

6) $\mu_8 := \{\zeta \in \mathbb{C} \mid \zeta^8 = 1\}$ (mit der Multiplikation)

7) $G := \langle (1\,2\,3\,4), (1\,3) \rangle$ 8) $H := \langle (1\,2\,3\,4), (2\,3) \rangle$

Lösung:
Die Quaternionengruppe enthält nur 1 Element der Ordnung 2 ($-E$), während die Diedergruppe D_8 neben der Spiegelung S noch die Drehung R_2 um π als Element der Ordnung 2 enthält, also $D_8 \not\simeq Q_8$.
D_8 und Q_8 sind nicht abelsch, die Gruppen 3)-6) sind abelsch. $\mu_8 = \{e^{\frac{2k\pi i}{8}} \mid 0 \leq k < 8\} = \langle e^{2\pi i/8} \rangle$ ist zyklisch von der Ordnung 8, also isomorph zu $\mathbb{Z}/8\mathbb{Z}$. Die Gruppen 3)–5) sind nicht untereinander isomorph, denn Gruppe 3) enthält ein Element der Ordnung 8, während Gruppe 4) den Exponenten 4 und Gruppe 5) den Exponenten 2 hat.
Die Gruppe 7) ist die Symmetriegruppe des regelmäßigen 4-Ecks (also des Quadrats) und daher isomorph zu D_8 (siehe Aufgabe 22). Gruppe 8) ist zu keiner der anderen Gruppen isomorph, da sie mehr als 8 Elemente enthält (leicht nachzurechnen). Genauer gilt: $H \simeq \mathcal{S}_4$, denn gemäß Aufgabe 20 ist $\langle (2\,3\,4\,1), (2\,3) \rangle = \mathcal{S}(\{2,3,4,1\} = \mathcal{S}_4$.
Zusammenfassend: Die einzigen Isomorphien sind die zwischen 1) und 7) sowie 3) und 6).

Aufgabe 31. (m)
Sei $G = \langle a \rangle$ zyklisch von der Ordnung n, ferner d ein Teiler von n. Zeigen Sie, dass G genau eine Untergruppe der Ordnung d enthält. Welche?

Lösung:
Nach Voraussetzung ist $m = \frac{n}{d} \in \mathbb{N}$. Für jede Untergruppe $H \leq G$ mit Ordnung d gilt:

$$a^k \in H \implies a^{kd} = e \iff \operatorname{ord} a = md \mid kd \iff m \mid k\,,$$

also $H \subset \langle a^m \rangle$. Andererseits gilt $\#\langle a^m \rangle = \operatorname{ord}(a^m) = d = \#H$, denn

$$e = a^{mk} \iff \operatorname{ord} a = n = md \mid mk \iff d \mid k\,.$$

Damit hat $\langle a^m \rangle$ die geforderte Ordnung d und stimmt mit H überein, ist also die einzige derartige Untergruppe der Ordnung d.

Aufgabe 32. (m)
Sei p eine Primzahl und G eine p-Gruppe, d. h. $\#G = p^k$ eine Potenz von p. G operiere auf der Menge Ω. Zeigen Sie für die Fixmenge $\Omega^G = \{a \in \Omega \mid \bigwedge_{\sigma \in G} \sigma a = a\}$:

$$\#\Omega \equiv \#(\Omega^G) \bmod p$$

Lösung:
Sei $\mathcal{B} := \{Ga \mid a \in \Omega\}$ die Menge aller Bahnen von Ω unter der Operation von G. Diese bilden eine disjunkte Zerlegung von Ω (siehe Prop. I.2.15) und die Bahnenlängen $\#Ga$ sind Gruppenindizes, also Teiler der Gruppenordnung $\#G$ und daher selbst p-Potenzen. Insbesondere $\#Ga = 1$ oder $p \mid \#Ga$. Nun gilt $\#Ga = 1 \iff Ga = \{a\} \iff \bigwedge_{\sigma \in G} \sigma a = a \iff a \in \Omega^G$. Damit ist $\Omega \setminus \Omega^G$ disjunkte Vereinigung der Bahnen B mit $\#B > 1$, d. h. mit $p \mid \#B$. Dann ist auch $\#\Omega - \#\Omega^G$ Vielfaches von p, wie behauptet.

Aufgabe 33. (s)
Die Kleinsche Vierergruppe $\mathcal{V}_4$ operiere auf der symmetrischen Gruppe $\mathcal{S}_4$ durch Konjugation. Bestimmen Sie die Bahnen.

Lösung:
Es sei $G := \mathcal{V}_4$ die operierende Gruppe und $\Omega := \mathcal{S}_4$ die Menge, auf der G durch Konjugation operiert. Für $a \in \mathcal{S}_4$ sei $a^G = \{a^\sigma \mid \sigma \in G\} = \{\sigma a \sigma^{-1} \mid \sigma \in G\}$. Wir erinnern an die Konjugationsformel für Zyklen in symmetrischen Gruppen: $\sigma(a\,b\,c\,\ldots)\sigma^{-1} = (\sigma a, \sigma b, \sigma c, \ldots)$ (siehe Aufgabe 20 b)). Konjugierte von Zyklen sind wieder Zyklen derselben Länge.
In $\Omega = \mathcal{S}_4$ gibt es neben der Identität und den 3 Produkten von 2 elementfremden Transpositionen (dies sind genau die Elemente in $\mathcal{V}_4$) nur noch Zyklen, nämlich

$$6 \text{ Transpositionen}, \qquad 8 \text{ 3-Zyklen}, \qquad 6 \text{ 4-Zyklen}.$$

$\mathcal{V}_4$ ist abelsch, also operiert G durch Konjugation auf sich selbst trivial: $a^G = \{a\}$ für alle $a \in \mathcal{V}_4$. Wir untersuchen nun die Operation von G auf den verschiedenen Zyklen. Nach der obigen Konjugationsformel ist die Wirkung von G auf den Zyklen unmittelbar ablesbar aus der Wirkung von $G = \mathcal{V}_4$ auf die Indexmenge $\underline{4} = \{1, 2, 3, 4\}$.
a^G für $a = (i\,j)$: Die Elemente in $\mathcal{V}_4$ sind gerade die Permutationen in $\mathcal{S}_4$, die *jede* der 3 möglichen disjunkten Zerlegungen von $\{1, 2, 3, 4\}$ in zwei 2-elementige Teilmengen in sich transformieren, also die beiden Teilmengen in sich abbilden oder vertauschen. Jede Transposition $a = (i\,j)$ bestimmt eine Zerlegung $\underline{4} = \{i, j\} \dot\cup \{k, l\}$. Für $\sigma \in G$ gilt also

$$\sigma(i\,j)\sigma^{-1} = (\sigma i, \sigma j) = \begin{cases} (i\,j) \\ (k\,l) \end{cases}, \quad (i\,j)^G = \{(i\,j), (k\,l)\}\,.$$

a^G besteht also genau aus $a = (i\,j)$ und der zu a elementfremden Transposition $b = (k\,l)$. Die Menge der 6 Transpositionen zerfällt unter der Operation von G in 3 Bahnen aus je zwei elementfremden Transpositionen.
a^G für $a = (1\,2\,3)$: $\sigma(1\,2\,3)\sigma^{-1} = (\sigma 1, \sigma 2, \sigma 3)$ hat den Fixpunkt $\sigma 4$. Für $\sigma \in G$ sind die $\sigma 4$ alle verschieden, also ist $\#a^G = 4$. Die 8 3-er Zyklen zerfallen in 2 G-Bahnen der Länge 4, wobei in jeder Bahn alle Fixpunkte vorkommen. 3-Zyklen mit gleichem Fixpunkt sind invers zueinander und liegen in verschiedenen G-Bahnen. Explizit:

$$a = (1\,2\,3) \implies a^G = \{(1\,2\,3), (2\,1\,4), (3\,4\,1), (4\,3\,2)\}\,, \quad (a^{-1})^G = (a^G)^{-1}\,.$$

a^G für $a = (i\,j\,k\,l)$: Es ist $\{i, j, k, l\} = \{1, 2, 3, 4\}$ und die nicht-trivialen Elemente von G wirken darauf durch jede mögliche Doppeltransposition:

$$(i\,j\,k\,l)^G = \{(i\,j\,k\,l)\,, (j\,i\,l\,k)\,, (k\,l\,i\,j)\,, (l\,k\,j\,i)\} = \{(i\,j\,k\,l), (l\,k\,j\,i)\}\,, \quad \text{also } a^G = \{a\,, a^{-1}\}\,.$$

Die 6 4-Zyklen zerfallen unter der Operation von G in 3 Bahnen, jeweils bestehend aus a und a^{-1}.
Fazit: G hat 4 Fixpunkte ($\mathcal{V}_4 \subset \Omega$), 3 Bahnen aus je zwei elementfremden Transpositionen, 2 Bahnen bestehend aus je 4 3-Zyklen, wobei eine Bahn gerade die Inversen der anderen Bahn sind, und schließlich 3 Bahnen jeweils bestehend aus einem 3-Zyklus und seinem Inversen.

Aufgabe 34. (s)
Sei G eine endliche Gruppe, p eine Primzahl, S_p eine p-Sylowgruppe von G und $N \lhd G$ ein Normalteiler. Zeigen Sie:

a) $S_p \cap N$ ist p-Sylowgruppe von N.

b) S_pN/N ist p-Sylowgruppe von G/N.

c) Ist N eine p-Untergruppe, so ist N in jeder p-Sylow-Untergruppe von G.

Lösung:
a) $S_p \cap N$ ist eine p-Untergruppe von N, also in einer p-Sylowgruppe N_p von N enthalten. Als p-Gruppe ist N_p in einer p-Sylowuntergruppe S_p^σ ($\sigma \in G$) von G enthalten:

$$S_p \cap N \subset N_p \subset S_p^\sigma \cap N \underset{N \lhd G}{=} (S_p \cap N)^\sigma \ .$$

Wegen $\#(S_p \cap N) = \#(S_p \cap N)^\sigma$ gilt überall Gleichheit, insbesondere ist $S_p \cap N = N_p$ eine p-Sylowgruppe von N.
b) Es ist $S_pN/N \simeq S_p/S_p \cap N$ (1. Isomorphiesatz), also S_pN/N eine p-Gruppe. Andererseits ist $(G/N : S_pN/N) = \frac{\#G}{\#S_pN} = (G : S_pN) \mid (G : S_p)$ kein Vielfaches von p und damit S_pN/N p-Sylowgruppe.
c) Die p-Gruppe N ist in einer p-Sylowgruppe S_p von G enthalten und für alle $\sigma \in G$ gilt dann $N = N^\sigma \subset S_p^\sigma$, N ist also in jeder p-Sylowuntergruppe von G enthalten (2. Sylowsatz).

Aufgabe 35. (s)
Es sei $G = \mathrm{GL}_n(\mathbb{R})$ und $M := M_n(\mathbb{R})$. Für $A \in M_n(\mathbb{R})$ bezeichne wie üblich A^t die transponierte Matrix. Zeigen Sie:

a) Durch $G \times M \ni (A, C) \mapsto A * C := ACA^\mathrm{t} \in M$ ist eine Operation von G auf $M_n(\mathbb{R})$ definiert.

b) Die Fixgruppe der Einheitsmatrix $E \in M$ unter dieser Operation ist die Gruppe $O_n(\mathbb{R})$ der orthogonalen Matrizen: $G_E = O_n(\mathbb{R})$.

c) Die Bahn von E unter dieser Operation ist die Menge aller positiv definiten symmetrischen Matrizen in $M_n(\mathbb{R})$. [Tipp: Diagonalisierbarkeit symmetrischer Matrizen.]

d)*Es sei $n = 2k$ gerade und $J_n = \begin{pmatrix} 0 & E_k \\ -E_k & 0 \end{pmatrix} \in M_n(\mathbb{R})$. Die Fixgruppe G_{J_n} von J_n unter dieser Operation ist die sog. reelle *symplektische* Gruppe. Zeigen Sie: Die Bahn von J_n unter der Operation von G ist die Menge aller *schiefsymmetrischen* Matrizen in $\mathrm{GL}_n(\mathbb{R})$. [Tipp: Zeigen Sie, dass man ausgehend von einer schiefsymmetrischen Matrix $C \in \mathrm{GL}_n(\mathbb{R})$ eine Basis (a_i) des $\mathbb{R}^n$ wählen kann mit folgenden Eigenschaften: a_1 ist ein (kanonischer) Einheitsvektor, $Ca_2 = a_1$ und $a_3, \ldots, a_n$ sind orthogonal zu Ca_1, Ca_2. Die Matrix A habe diese Vektoren als Zeilen. Untersuchen Sie die Form von ACA^t und führen Sie diese Überlegungen dann induktiv weiter.]

Lösung:
a) $E * C = C$ ist klar, ebenso $AB * C = ABC(AB)^\mathrm{t} = A \cdot BCB^\mathrm{t} \cdot A^\mathrm{t} = A * (B * C)$.
b) $A \in G_E \iff AEA^\mathrm{t} = E \iff AA^\mathrm{t} = E \iff A \in O_n(\mathbb{R})$.
c) $C \in G * E \iff \bigvee_{A \in \mathrm{GL}_n(\mathbb{R})} C = AA^\mathrm{t} \implies C \in \mathrm{GL}_n(\mathbb{R})$ symmetrisch. Daraus folgt die Existenz einer Orthonormalbasis des euklidischen Raumes $\mathbb{R}^n$ aus Eigenvektoren von C (siehe Lineare Algebra). Sämtliche Eigenwerte von $C = AA^\mathrm{t}$ sind positiv und C daher positiv definit:

$$Cv = \lambda v \implies \lambda |v|^2 = \langle Cv, v\rangle = \langle AA^\mathrm{t}v, v\rangle = \langle A^\mathrm{t}v, A^\mathrm{t}v\rangle = \left|A^\mathrm{t}v\right|^2 \implies \lambda > 0\,.$$

Sei nun umgekehrt C eine symmetrische positiv definite Matrix in M. Wegen der Symmetrie existiert eine ONB aus Eigenvektoren von C, also eine orthogonale Matrix T mit $T^{-1}CT = diag(\lambda_1, \ldots, \lambda_n)$. Die Diagonalelemente λ_i sind gerade die Eigenwerte von C und daher nach Voraussetzung positiv, also $\lambda_i = \alpha_i^2$ mit $\alpha_i \in \mathbb{R}_+$. Also gilt mit der Diagonalmatrix $S = diag(\alpha_1, \ldots, \alpha_n) \in G$:

$$T^{-1}CT = S^2 \iff C = TS^2T^{-1} = TS \cdot ST^\mathrm{t} = TS \cdot (TS)^\mathrm{t} \in G * E\,.$$

d) Mit J_n ist auch $A * J_n = AJ_nA^{\mathrm{t}}$ schiefsymmetrisch. Außerdem ist $\det(A * J_n) = \det J_n \cdot (\det A)^2 \neq 0$, also $A * J_n \in \mathrm{GL}_n(\mathbb{R})$.
Sei nun umgekehrt $C \in \mathrm{GL}_n(\mathbb{R})$ schiefsymmetrisch. Dann gilt zunächst für alle $v, w \in \mathbb{R}^n$

$$(1) \quad \langle v, Cw\rangle = -\langle w, Cv\rangle\,, \qquad (2) \quad Cv \perp v\,.$$

Denn: $\langle v, Cw\rangle = v^{\mathrm{t}}Cw = w^{\mathrm{t}}C^{\mathrm{t}}v = w^{\mathrm{t}}(-C)v = -\langle w, Cv\rangle$ und insbesondere $\langle v, Cv\rangle = -\langle v, Cv\rangle$.

Vorüberlegung gemäß dem Tipp: Wir wählen einen (kanonischen) Einheitsvektor $a_1 \in \mathbb{R}^n$ und $a_2 := C^{-1}a_1$ (C regulär). Dann gilt nach (2) $a_1 = Ca_2 \perp a_2$ und $a_1, a_2 (\neq 0)$ sind daher linear unabhängig. Da C regulär ist, ist $U := \mathbb{R}Ca_1 \oplus \mathbb{R}Ca_2$ 2-dimensional und das orthogonale Komplement

$$W := U^{\perp} = \{w \in \mathbb{R}^n \mid \bigwedge_{u \in U} \langle w, u\rangle = 0\} = \{w \in \mathbb{R}^n \mid \langle u, Ca_1\rangle = 0 = \langle u, Ca_2\rangle\}$$

hat daher die Dimension $n - 2 = 2(k-1)$. Sei $a_3, \ldots, a_n$ eine beliebige Basis von W. Dann ist $A^{\mathrm{t}} := (a_1|a_2|a_3|\ldots|a_n) \in \mathrm{GL}_n(\mathbb{R})$ und es gilt (wobei wir 0-Blöcke der Übersichtlichkeit wegen nicht ausfüllen)

$$A * C = ACA^{\mathrm{t}} = \left(\begin{array}{cc|c} 0 & 1 & \\ -1 & 0 & \\ \hline & & C_{k-1} \end{array}\right) \quad \text{mit } C_{k-1} \in M_{2(k-1)}(\mathbb{R})\,.$$

Beweis: Die Koeffizienten von $A * C$ sind $\alpha_{ij} = a_i^{\mathrm{t}}Ca_j = \langle a_i, Ca_j\rangle \underset{(1)}{=} -\alpha_{ji}$ und es gilt:

$$\begin{aligned}
&\alpha_{ii} = \langle a_i, Ca_i\rangle \underset{(2)}{=} 0\,,\\
&\alpha_{12} = \langle a_1, Ca_2\rangle = \langle a_1, a_1\rangle = 1\,,\ \alpha_{21} \underset{(1)}{=} -\alpha_{12} = -1\\
&1 \le i \le 2\,,\ 3 \le j \le n \implies a_j \perp Ca_i \implies \alpha_{ji} = 0 = \alpha_{ij}\,.
\end{aligned}$$

Aufgrund dieser Vorüberlegungen kann man nun induktiv zeigen:

$$\bigwedge_{k \in \mathbb{N}_+} \bigwedge_{\substack{C \in \mathrm{GL}_{2k}(\mathbb{R})\\ \text{schiefsymmetrisch}}} \bigvee_{A \in \mathrm{GL}_{2k}(\mathbb{R})} ACA^{\mathrm{t}} = \left(\begin{array}{cc|c|cc} 0 & 1 & & & \\ -1 & 0 & & & \\ \hline & & \ddots & & \\ \hline & & & 0 & 1 \\ & & & -1 & 0 \end{array}\right) =: H_k$$

Beweis: Sei $k \in \mathbb{N}_+$ und $C \in \mathrm{GL}_{2k}(\mathbb{R})$ schiefsymmetrisch. Wir wählen A wie in der Vorüberlegung. Ist $k = 1$, so ist der Beweis fertig. Für $k > 1$ wenden wir nun die Induktionsvoraussetzung auf die Matrix C_{k-1} an. Dies ist möglich, denn mit C und ACA^{t} ist auch C_{k-1} schiefsymmetrisch und wegen $\det ACA^{\mathrm{t}} = \det H_1 \cdot \det C_{k-1}$ ist C_{k-1} auch regulär. Also existiert zu $C_{k-1} \in \mathrm{GL}_{2(k-1)}(\mathbb{R})$ eine Matrix $A_{k-1} \in \mathrm{GL}_{2(k-1)}(\mathbb{R})$ mit $A_{k-1}C_{k-1}A_{k-1}^{\mathrm{t}} = H_{k-1}$. Wir erweitern nun A_{k-1} zu

$$B := \left(\begin{array}{cc|c} 1 & 0 & \\ 0 & 1 & \\ \hline & & A_{k-1} \end{array}\right) \in \mathrm{GL}_{2k}(\mathbb{R})$$

und erhalten

$$\begin{aligned}
B(ACA^{\mathrm{t}})B^{\mathrm{t}} &= \left(\begin{array}{cc|c} 1 & 0 & \\ 0 & 1 & \\ \hline & & A_{k-1} \end{array}\right)\left(\begin{array}{cc|c} 0 & 1 & \\ -1 & 0 & \\ \hline & & C_{k-1} \end{array}\right)\left(\begin{array}{cc|c} 1 & 0 & \\ 0 & 1 & \\ \hline & & A_{k-1}^{\mathrm{t}} \end{array}\right)\\
&= \left(\begin{array}{cc|c} 0 & 1 & \\ -1 & 0 & \\ \hline & & A_{k-1}C_{k-1}A_{k-1}^{\mathrm{t}} \end{array}\right) = \left(\begin{array}{cc|c} 0 & 1 & \\ -1 & 0 & \\ \hline & & H_{k-1} \end{array}\right) = H_k
\end{aligned}$$

Damit ist die Induktion vollständig. Für jede reguläre schiefsymmetrische Matrix $C \in \mathrm{GL}_{2k}(\mathbb{R})$ gilt daher $H_k \in G * C$, also $C \in G * H_k$. Dies bedeutet, dass die Bahn $G * H_k$ alle regulären schiefsymmetrischen Matrizen enthält, insbesondere auch J_{2k}, und es folgt

$$G * J_{2k} = G * H_k = \{C \in \mathrm{GL}_{2k}(\mathbb{R}) \mid C^{\mathrm{t}} = -C\}\,.$$

Algebra I
Übung 7

Aufgabe 36. (m)
Sei G eine Gruppe, $H \leq G$ Untergruppe und $\mathcal{N}_G(H) := \{\sigma \in G \mid \sigma H \sigma^{-1} = H\}$ der sog. *Normalisator* von H in G. Zeigen Sie:

a) $H \leq \mathcal{N}_G(H) \leq G$.

b) Für $G' \leq G$ gilt: $H \lhd G' \iff H \subset G' \subset \mathcal{N}_G(H)$.

c) Die Anzahl der verschiedenen Konjugierten $\sigma H \sigma^{-1}$ ($\sigma \in G$) von H in G ist gleich dem Index $(G : \mathcal{N}_G(H))$ des Normalisators in G.

Lösung:
a) Sei $h \in H$. Dann gilt $hHh^{-1} \subset H$ und $h^{-1}Hh \subset H \implies H \subset hHh^{-1}$, insgesamt also $hHh^{-1} = H$, $h \in \mathcal{N}_G(H)$.
Sind $h_1, h_2 \in \mathcal{N}_G(H)$, so gilt $h_i H h_i^{-1} = H$, $h_i^{-1} H h_i = H^{-1} = H$ und daher $h_1 h_2^{-1} H h_2 h_1^{-1} = H$, also $h_1 h_2^{-1} \in \mathcal{N}_G(H)$ und nach dem Untergruppenkriterium daher $\mathcal{N}_G(H) \leq G$.
b) $H \lhd G' \iff H \subset G' \wedge \bigwedge_{\sigma \in G'} \sigma H \sigma^{-1} = H \iff H \subset G' \subset \mathcal{N}_G(H)$.
c) G operiert durch Konjugation auf den Elementen, aber auch auf den Teilmengen von G. Unter dieser Operation ist die Bahn von H gerade die Menge aller Konjugierten von H und die Fixgruppe von H ist $\mathrm{Fix}_G(H) = \{\sigma \in G \mid \sigma H \sigma^{-1} = H\} = \mathcal{N}_G(H)$. Also folgt nach der Bahnengleichung Prop. I.2.15 c) die Behauptung.

Aufgabe 37. (m)
Es sei p ein Primzahl, G eine Gruppe mit $\#G = p^s m$ mit $s, m \in \mathbb{N}_+$ und $p \nmid m$. Zeigen Sie:

a) Für die Anzahl s_p der p-Sylowgruppen von G gilt $s_p \mid m$. [Tipp: Aufgabe 36.]

b) Ist $m < p$, so gibt es genau eine p-Sylowgruppe in G und diese ist Normalteiler.

Lösung:
a) Wegen $p \mid \#G$ gibt es eine p-Sylowgruppe P in G. Alle p-Sylowgruppen von G sind untereinander konjugiert (Zweiter Sylowsatz). Ihre Anzahl s_p ist also die Anzahl der Konjugierten von P, nach Aufgabe 36 also gleich dem Index $(G : \mathcal{N}_G(P))$ des Normalisators von P. Wegen $P \leq \mathcal{N}_G(P)$ folgt $s_p = (G : \mathcal{N}_G(P)) \mid (G : P) = m$.
b) Ist $m < p$, so ist $1 \leq s_p < p$ und wegen $s_p \equiv 1 \bmod p$ (Erster Sylowsatz) folgt $s_p = 1$: Es gibt nur eine p-Sylowgruppe in G, die also mit allen ihren Konjugierten übereinstimmen muss und daher ein Normalteiler in G ist.

Aufgabe 38. (s)
Sei G eine endliche Gruppe und $Z := \mathrm{Zentr}(G)$ ihr Zentrum. Zeigen Sie:

a) Ist G/Z zyklisch, so ist G abelsch.

b) Ist G eine nicht-abelsche Gruppe der Ordnung p^3, p eine Primzahl, so stimmen Zentrum Z und Kommutatorgruppe $[G, G]$ von G überein. [Tipp: p-Gruppen haben ein nicht-triviales Zentrum.]

Lösung:
a) Es ist nach Voraussetzung $G/Z = \langle \bar{\sigma} \rangle$ 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 $ba = z'\sigma^j \cdot z\sigma^i = zz'\sigma^{i+j}$. Also $ab = ba$ für alle $a, b \in G$.

b) Da G eine nicht-abelsche p-Gruppe ist, gilt $\{e\} \neq Z \neq G$, also $1 < \#Z = p^k < \#G = p^3$. Es gibt also nur zwei Fälle: $\#Z = p$ oder $\#Z = p^2$. Der letztere Fall ist nicht möglich, da sonst G/Z primzyklisch und G dann nach a) abelsch wäre. Also ist $\#Z = p$ und $\bar{G} = G/Z$ eine Gruppe der Ordnung p^2. Auf $\bar{G}$ kann man nun erneut a) anwenden ($\bar{G}/\mathrm{Zentr}\,\bar{G}$ ist zyklisch) und folgern, dass $\bar{G}$ abelsch ist. Also enthält Z die Kommutatorgruppe $[G, G]$ (siehe Bemerkung I.4.6). Wäre $[G, G] = \{e\}$, so wäre G abelsch, Wid. Somit folgt $Z = [G, G]$.

Aufgabe 39. (s)
Zeigen Sie: Gruppen der Ordnung 56 sind nicht einfach.
[Tipp: Zur Bestimmung der Anzahl der Sylowgruppen von G zähle man in einem Falle die Elemente der Ordnung $\neq 7$ ab.]

Lösung:
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 nur 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.

Aufgabe 40. (s)
Seien p, q verschiedene Primzahlen. Zeigen Sie, dass alle Gruppen der Ordnung p^2q auflösbar sind. [Tipp: Untersuchen Sie die Anzahl der Sylowgruppen.]

Lösung:
Sind s_p, s_q die Anzahlen der p- bzw. q-Sylowgruppen von G, so gilt nach dem 2. Sylowsatz d)

$$s_p \equiv 1 \bmod p\,,\ s_p \mid q\,, \quad s_q \equiv 1 \bmod q\,,\ s_q \mid p^2\,.$$

1. Fall $\underline{q < p}$: Wäre $s_p \neq 1$, so folgte $s_p = q \equiv 1 \bmod p$, also $p \mid q - 1 < p$, Wid. Also ist $s_p = 1$ und G enthält nur eine p-Sylowgruppe S_p, die daher ein Normalteiler ist. Es ist G/S_p von der Ordnung q, also primzyklisch. S_p muss als Gruppe der Ordnung p^2 abelsch sein, denn andernfalls hätte S_p ein Zentrum der Ordnung p, so dass nach Aufgabe 38 a) S_p dann doch abelsch sein müsste. In diesem 1. Fall sind also S_p und G/S_p und daher auch G auflösbar (siehe Aufgabe 41).
2. Fall $\underline{p < q}$: Ist $s_q = 1$, so argumentiert man wie oben: $S_q \lhd G$ und S_q ist primzyklisch. G/S_q hat die Ordnung p^2 und ist daher wie oben gezeigt abelsch. Also ist G auflösbar.
Sei nun $s_q \neq 1$, also ist $s_q - 1 \in \mathbb{N}_+$ Vielfaches von q und daher $s_q > q > p$. Also folgt

$$s_q = p^2 \implies p^2 \equiv 1 \bmod q \implies q \mid p^2 - 1 = (p+1)(p-1) \iff q \mid p-1 \ \vee\ q \mid p+1\,.$$

Wegen $p < q$ kommt nur $q \mid p + 1$, also $q = 3, p = 2$ in Frage. Es ist also G eine Gruppe der Ordnung 12 und $s_3 = 4$. In den 4 verschiedenen 3-Sylowgruppen gibt es dann $4 \cdot 2 = 8$ Elemente der Ordnung 3 und in G dann nur 4 Elemente von 2-Potenzordnung. G kann also nur eine 2-Sylowgruppe (der Ordnung 4) enthalten und es ist $s_p = s_2 = 1$. Wieder folgt die Auflösbarkeit.

Aufgabe 41. (s)
Zeigen Sie:

a) Jede Untergruppe H einer auflösbaren Gruppe G ist auflösbar.

b) Jedes homomorphe Bild G' einer auflösbaren Gruppe G ist auflösbar.

c) Ist G eine Gruppe und $N \lhd G$ ein Normalteiler, so gilt:

$$G \text{ auflösbar} \iff N \text{ und } G/N \text{ auflösbar.}$$

Lösung:
a) G besitzt eine Normalreihe (G_i) mit abelschen Faktoren. Der Durchschnitt aller Glieder der Normalreihe von G mit einer beliebigen Untergruppe H liefert eine Normalreihe von H. Deren Faktoren sind Untergruppen der Faktoren von G:

$$G_i \cap H / G_{i+1} \cap H \hookrightarrow G_i / G_{i+1}\,, \quad h(G_{i+1} \cap H) \mapsto h G_{i+1}\,.$$

und daher selbst abelsch.
b) Unter einem Epimorphismus $\varphi : G \twoheadrightarrow G'$ wird eine Normalreihe von G auf eine Normalreihe von G' abgebildet: $G_{i+1} \lhd G_i \implies \varphi(G_{i+1}) \lhd \varphi(G_i)$. Deren Faktoren sind epimorphe Bilder der Faktoren von G:

$$\bar{\varphi} : G_i / G_{i+1} \twoheadrightarrow \varphi(G_i) / \varphi(G_{i+1})$$

und daher ebenfalls abelsch.
c) Es ist nur noch $\Leftarrow$ zu zeigen. Man wähle eine Normalreihe $\mathfrak{g}_i$ in $\mathfrak{g} = G/N$ und bilde die vollen Urbilder $\nu^{-1}(\mathfrak{g}_i)$ in G. Dies ergibt eine Normalreihe von G hinunter bis $\nu^{-1}(\{\bar{e}\}) = \operatorname{Ke}\nu = N$. Zusammen mit einer Normalreihe von N erhält man eine vollständige Normalreihe von G. Deren Faktoren sind Faktoren in der Normalreihe von N (und daher abelsch) oder isomorph zu Faktoren der Normalreihe von $\mathfrak{g} = G/N$ (Isomorphiesatz (1.20) d)), und daher ebenfalls abelsch.

Algebra I
Übung 8

Aufgabe 42. (m)
Formulieren und beweisen Sie für Ringe und Moduln Homomorphie- und Isomorphiesätze entsprechend den Sätzen aus der Gruppentheorie.

Lösung:
Für Ringe siehe Vorlesung Satz II.1.7 (S. 36) 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. 35). 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 43. (m)
Sei R ein kommutativer, unitärer Ring, $(R^{\mathbb{N}}, +, .)$ der R-Modul der R-wertigen Funktionen auf $\mathbb{N}$ (Folgen) mit wertweise definierter Addition $+$ und skalarer Multiplikation $r.\ldots$ ($r \in R$). Außerdem sei $*$ die in der Vorlesung definierte Multiplikation $(a * b)_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{i+j=n} a_i b_j$ ($n \in \mathbb{N}$) (siehe Beispiele II.1.2 (5)). Zeigen Sie:

a) $S = (R^{\mathbb{N}}, +, *)$ ist ein kommutativer Ring mit Einselement $e = (1, 0, 0, \ldots) = (\delta_{0n})_{n\in\mathbb{N}}$. Durch $r \mapsto r.e$ wird R in S eingebettet.

b) Setzt man $X := (0, 1, 0, 0, \ldots) = (\delta_{1i})_{i\in\mathbb{N}}$, so gilt

$$X^k := \underbrace{X * \ldots * X}_{k \text{ Faktoren}} = (0, \ldots, 0, \underset{\substack{\uparrow \\ k}}{1}, 0, \ldots) = (\delta_{kn})_{n\in\mathbb{N}}\,.$$

c) Der von R und X in S erzeugte Unterring $R[X] = \{\sum_{k=0}^{m} r_k X^k \mid m \in \mathbb{N}\,,\ r_0, \ldots, r_m \in R\}$ ist gleich der Menge der 'endlichen' Folgen $E := \{a \in R^{\mathbb{N}} \mid a_n = 0 \text{ für fast alle } n \in \mathbb{N}\}$.

d) $R[X]$ ist Polynomring über R in einer Unbestimmten X.

Lösung:
$*$ ist offensichtlich kommutativ und distributiv. Zur Assoziativität:

$$(a * b) * c = (\sum_{i+j=m} a_i b_j)_m * (c_n)_n = (\sum_{m+n=k} \sum_{i+j=m} a_i b_j c_n)_k = (\sum_{i+j+n=k} a_i b_j c_n)_k = a * (b * c)\,.$$

$e = (\delta_{0n})_n$ ist Einselement: $e * a = (\sum_{n=0}^{k} \delta_{0n} a_{k-n})_k = (a_k)_k = a$, und die Abbildung $r \mapsto r.e$ ist offensichtlich injektiv: $(0, 0, \ldots) = r.e = (r, 0, 0, \ldots) \implies r = 0$.
b) Induktiv: $X^0 = e = (\delta_{0n})_n$ und

$$X^k = (\delta_{ki})_i \implies X^k * X = (\sum_{i+j=n} \underbrace{\delta_{ki}}_{\neq 0 \Leftrightarrow i=k} \underbrace{\delta_{1j}}_{\neq 0 \Leftrightarrow j=1})_n = (\delta_{k+1,n})_n\,.$$

c) $R[X] \subset E$ ist klar, denn für $a = \sum_{k=0}^{m} r_k X^k \in R[X]$ gilt

$$n > m \implies a_n = (\sum_{k=0}^{n} r_k X^k)_n = \sum_{k=0}^{m} r_k \delta_{kn} \underset{k\le m<n}{=} 0\,, \text{ also } a \in E\,.$$

Ist umgekehrt $a \in E$, etwa $a_n = 0$ für $n > m$, so ist $b = \sum_{k=0}^{m} a_k X^k \in R[X]$ und es gilt

$$b_n = (\sum_{k=0}^{m} a_k X^k)_n = \sum_{k=0}^{m} a_k \delta_{kn} = \begin{cases} a_n & n \le m \\ 0 = a_n & n > m \end{cases} = a_n\,, \text{ also } a = b \in R[X]\,.$$

d) $R[X]$ ist ein kommutativer Ring mit Eins, er enthält X und jedes $f = \sum_{k=0}^{m} a_k X^k \in R[X]$ bestimmt seine Koeffizienten a_k eindeutig, denn (siehe c)) $f_n = a_n$, also ist der Koeffizient a_n gleich dem n-ten Folgenglied f_n von $f \in R^{\mathbb{N}}$ und damit durch f eindeutig bestimmt.

Aufgabe 44. (s)
Sei M eine nicht-leere Menge und $R := \mathcal{P}(M)$ die Potenzmenge. Für $A \subset M$ sei $\tilde{A} = M \setminus A$ das mengentheoretische Komplement. Wir definieren auf R zwei Verknüpfungen

$$A \cdot B := A \cap B\,, \qquad A + B := (A \cap \tilde{B}) \cup (\tilde{A} \cap B)\,.$$

Zeigen Sie:

a) $(R, +, \cdot)$ ist ein kommutativer unitärer Ring.

b) Wie muss M beschaffen sein, damit R nullteilerfrei ist?

c) Ist R nullteilerfrei, so ist R ein Körper.

Lösung:
a) Nach den de Morganschen Regeln gilt $A\widetilde{+}B = (\tilde{A} \cup B) \cap (A \cup \tilde{B}) = A \cap B \ \cup \ \tilde{A} \cap \tilde{B}$ und daher

$$\begin{aligned}(A+B)+C &= [A \cap \tilde{B} \ \cup \ \tilde{A} \cap B] \cap \tilde{C} \ \cup \ [A \cap B \ \cup \ \tilde{A} \cap \tilde{B}] \cap C \\ &= A \cap \tilde{B} \cap \tilde{C} \ \cup \ \tilde{A} \cap B \cap \tilde{C} \ \cup \ A \cap B \cap C \ \cup \ \tilde{A} \cap \tilde{B} \cap C\,.\end{aligned}$$

$(A+B)+C$ besteht also aus genau den Elementen $x \in M$, die entweder in allen drei Mengen liegen oder in genau einer der drei Mengen. Diese Symmetrie der letzten Formel zeigt $(B+C)+A = (A+B)+C$, so dass mit der offensichtlichen Kommutativität von $+$ die Assoziativität folgt.
Die Kommutativität und Assoziativität von $\cdot$ ist klar. Zur Distributivität:

$$\begin{aligned}(A+B)C &= [(A \cap \tilde{B} \ \cup \ (\tilde{A} \cap B)] \ \cap \ C = A \cap \tilde{B} \cap C \ \cup \ \tilde{A} \cap B \cap C\,, \\ AC + BC &= A \cap C \cap (\tilde{B} \cup \tilde{C}) \ \cup \ (\tilde{A} \cup \tilde{C}) \cap B \cap C = A \cap \tilde{B} \cap C \ \cup \ \tilde{A} \cap B \cap C\,.\end{aligned}$$

[Sprachlich logische Argumentation: $A+B$ besteht aus den Elementen, die in einer, aber nicht beiden Mengen liegen: $A+B = (A \cup B) \setminus (A \cap B)$. $A\widetilde{+}B$ besteht also aus den Elementen, die in beiden oder keiner der Mengen liegen: $A\widetilde{+}B = A \cap B \cup \tilde{A} \cap \tilde{B}$. Daher besteht $(A+B)+C$ aus genau den Elementen, die in genau einer der beiden Mengen $A+B$, C liegen, also in genau einer der Mengen A, B und nicht in C liegen $((A \cap \tilde{B} \cap \tilde{C}) \cup (\tilde{A} \cap B \cap \tilde{C}))$ oder in C liegen, sowie in A *und* B oder weder in A noch in B $((A \cap B \cap C) \cup (\tilde{A} \cap \tilde{B} \cap C))$.
$(A+B)C$ besteht aus allen Elementen, die in C und genau einer der Mengen A, B liegen. $AB + AC$ besteht aus allen Elementen, die in genau einem der Durchschnitte $A \cap C$, $B \cap C$, also notwendig in C und genau einer der Mengen A, B liegen. Dies beweist die Distributivität.]
Nullelement des Ringes ist die leere Menge $\emptyset$ und Negatives von A ist A selbst: $A+A = A \cap \tilde{A} = \emptyset$. Einselement ist die Gesamtmenge M: $M \cdot A = M \cap A = A$.
b) R ist nullteilerfrei, wenn $A \cap B = \emptyset \implies A = \emptyset \vee B = \emptyset$. Ist M einelementig, so gilt dies. gibt es jedoch zwei verschiedene Elmente $a, b \in M$, so sind $A = \{a\}$ und $B = \{b\}$ echte Nullteiler.
c) Ist R nullteilerfrei, also M einelementig, so ist $R = \{\emptyset, M\} = \{0, 1\}$ der Körper von 2 Elementen.

Aufgabe 45. (s)
Sei R ein kommutativer Ring mit Eins. Zeigen Sie: R ist genau dann ein Körper, wenn R keine Ideale $(0) \neq \mathfrak{a} \neq R$ enthält.

Lösung:
Sei R ein Körper und $(0) \neq \mathfrak{a} \lhd R$ ein nicht-triviales Ideal. Dann existiert $0 \neq a \in \mathfrak{a}$. Dann enthält $\mathfrak{a}$ die 1: $1 = a^{-1} \cdot a \in Ra \subset \mathfrak{a}$, und ist daher gleich R: $R = R \cdot 1 \subset \mathfrak{a}$, jedes nicht-triviale Ideal ist gleich R.
Umgekehrt: Ist $0 \neq a \in R$, so ist $Ra \lhd R$, nach Voraussetzung also $Ra = R$ und damit $1 \in Ra$, also $1 = ba$ für ein $b \in R$. Jedes $a \neq 0$ besitzt also ein Inverses, R ist ein Körper.

Aufgabe 46. (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) Für eine sog. *kurze exakte Sequenz*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

gilt:

$$M' \simeq f(M') \quad \text{und} \quad M/f(M') \simeq M''\,.$$

c) 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) 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:

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

c) 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 47. (s)
Seien M und M_i $(i = 1, \ldots, n)$ Moduln über einem Ring. Zeigen Sie die Äquivalenz der folgenden Aussagen:

a) $M \simeq M_1 \times \ldots \times M_n$.

b) Es gibt für $i = 1, \ldots, n$ Homomorphismen $\varphi_i : M_i \to M$ und $\psi_i : M \to M_i$ mit

$$\psi_j \circ \varphi_i = \begin{cases} \mathrm{id}_{M_i} & i = j \\ 0 & i \neq j \end{cases} \quad \text{und} \quad \sum_{i=1}^{n} \varphi_i \circ \psi_i = \mathrm{id}_M \qquad (*)$$

[Tipp: Studieren Sie zunächst den Sonderfall $M = M_1 \times \ldots \times M_n$.]
Lösung:
a) $\Rightarrow$ b): Im Sonderfall $M = M_1 \times \ldots \times M_n$ erfüllen die kanonischen Einbettungen $\iota_i : M_i \to M$, $x_i \mapsto (0, \ldots, 0, x_i, 0, \ldots, 0)$ und die Projektionen $\pi_i : M \to M_i$, $(x_1, \ldots, x_n) \mapsto x_i$ die Eigenschaften $(*)$. Im allgemeinen Fall seien $\varphi : M_1 \times \ldots \times M_n \xrightarrow{\sim} M$ und $\psi : M \xrightarrow{\sim} M_1 \times \ldots \times M_n$ zueinander inverse Isomorphismen und wir setzen $\varphi_i = \varphi \circ \iota_i : M_i \to M$ sowie $\psi_i = \pi_i \circ \psi$. Dann erfüllen diese Homomorphismen die Eigenschaft $(*)$.
b) $\Rightarrow$ a): Sind φ_i und ψ_i mit $(*)$ gegeben, so sind die Abbildungen

$$\varphi := \sum_{i=1}^{n} \varphi_i \circ \pi_i : M_1 \times \ldots \times M_n \to M \quad \text{und} \quad \psi := (\psi_1, \ldots, \psi_n) : M \to M_1 \times \ldots \times M_n$$

zueinander inverse Homomorphismen:

$$\varphi \circ \psi(x) = \varphi(\psi_1(x), \ldots, \psi_n(x)) = \sum_{i=1}^{n} \varphi_i(\psi_i(x)) = x\,,$$

$$\psi \circ \varphi(x_1, \ldots, x_n) = \psi(\sum_{i=1}^{n} \varphi_i(x_i)) = (\sum_{i=1}^{n} \psi_1 \circ \varphi_i(x_i), \ldots, \sum_{i=1}^{n} \psi_n \circ \varphi_i(x_i)) = (x_1, \ldots, x_n)\,.$$

Algebra I
Übung 9

Aufgabe 48. (m)
E sei eine Teilmenge eines Ringes R. Beschreiben Sie die erzeugten Unterstrukturen $[E]$, ${}_R\langle E\rangle$, $\langle E\rangle_R$ und ${}_R\langle E\rangle_R$ durch ihre Elemente.

Lösung:
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.

Begründungen: Da die linke Seite jeweils die Elemente der rechten Seite enthalten muss, muss man nur nachrechnen, dass die jeweilige rechte Seite eine entsprechende Unterstruktur von R ist, also gegen die jeweiligen Operationen $+$, $-$ sowie $\cdot$ im Ringfall bzw. Multiplikation mit Ringelementen $r\cdot$ (im Fall der Ideale) abgeschlossen ist.

Aufgabe 49. (m)
Sei R ein Integritätsbereich.

a) Wiederholen Sie aus der Vorlesung die Konstruktion des Quotientenkörpers $\mathrm{Quot}(R)$.

b) Zeigen Sie: Ist R in einem Körper K enthalten, so ist

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

der kleinste R umfassende Teilkörper von K, und dieser ist isomorph zum Quotientenkörper $\mathrm{Quot}(R)$.

Lösung:
b) Offenbar ist $R \subset (R)$ und jeder R umfassende Teilkörper von K muss das angegebene (R) enthalten. Es bleibt zu zeigen, dass (R) ein Körper ist. Als Teilmenge eines Körpers genügt es zu zeigen, dass (R) 0 und 1 enthält (klar, ganz R ist enthalten) und abgeschlossen ist gegen $+$, $-$, $\cdot$ sowie Inversenbildung für die von 0 verschiedenen Elemente. Dies rechnet man leicht nach (Bruchrechnung!).
Die Zuordnung $\mathrm{Quot}(R) \ni \frac{a}{b} \mapsto ab^{-1} \in (R)$ $(a, b \in R, b \neq 0)$ ist wohldefiniert und injektiv:

$$\frac{a}{b} = \frac{x}{y} \in \mathrm{Quot}(R) \iff ay = xb \in R \iff ab^{-1} = xy^{-1} \in (R) .$$

Die Surjektivität ist offensichtlich und die Homomorphie wieder eine Folge der Bruchrechnung.

Aufgabe 50. (m)
Sei $f : R \to R'$ ein Ringhomomorphismus und $\mathfrak{a}'$ ein Ideal in R'. Zeigen Sie:

a) Ist $\mathfrak{a}'$ Primideal in R', so ist $f^{-1}(\mathfrak{a}')$ Primideal in R.

b) Ist f ein Epimorphismus und $\mathfrak{a}'$ maximal in R', so ist $f^{-1}(\mathfrak{a}')$ maximal in R.

Lösung:
$\mathfrak{a} := f^{-1}(\mathfrak{a}')$ ist ein Ideal in R und es gilt nach den Homomorphiesätzen

$$R/\mathfrak{a} = R/f^{-1}(\mathfrak{a}') \hookrightarrow R'/\mathfrak{a}'\,.$$

a) $\mathfrak{a}'$ Primideal in $R' \iff R'/\mathfrak{a}'$ nullteilerfrei. Dann ist auch $R/\mathfrak{a} \hookrightarrow R'/\mathfrak{a}'$ nullteilerfrei und $\mathfrak{a}$ ein Primideal in R.
b) Es ist nach Voraussetzung $f(R) = R'$ und daher $R/\mathfrak{a} \simeq R'/\mathfrak{a}'$, also

$$\mathfrak{a}' \lhd R' \text{ maximal } \iff R'/\mathfrak{a}' \simeq R/\mathfrak{a} \text{ Körper } \iff \mathfrak{a} \lhd R \text{ maximal}\,.$$

Aufgabe 51. (s)
Sei R ein kommutativer unitärer Ring. R heißt *lokaler* Ring, wenn R genau ein maximales Ideal besitzt. Zeigen Sie:

a) R ist genau dann lokaler Ring, wenn die Menge $N = R \setminus R^\times$ der Nichteinheiten ein Ideal in R ist.

b) Ist für jedes $x \in R$ entweder x oder $1 - x$ eine Einheit, so ist R ein lokaler Ring.

c) Ist K ein Körper und $R = K[[X]]$ der formale Potenzreihenring über K (vgl. Beispiele II.1.2 (5) bzw. Aufgabe 43 a)), so gilt:

$$(a_0, a_1, \ldots) \in R^\times \iff a_0 \in K^\times$$

und $K[[X]]$ ist ein lokaler Ring.

Lösung:
a) $\Leftarrow$: Ein echtes Ideal kann keine Einheit enthalten und ist daher in $N = R \setminus R^\times$ enthalten. Da N ein Ideal ist, ist es das einzige maximale Ideal.
$\Rightarrow$: Das maximale Ideal $\mathfrak{m}$ ist in N enthalten. Umgekehrt erzeugt jede Nichteinheit $a \in N$ ein echtes Ideal $Ra \lhd R$, welches in dem einzigen maximalen Ideal $\mathfrak{m}$ enthalten sein muss: $N \subset \mathfrak{m}$. Zusammengenommen ist also $N = \mathfrak{m} \lhd R$ ein Ideal.
b) Für $r, x \in R$ gilt $rx \in R^\times \implies x \in R^\times$ und daher $r \cdot N \subset N$ für alle $r \in R$. Bleibt zu zeigen, dass N additiv abgeschlossen ist: Seien also $x, y \in N$ und angenommen $x + y \notin N$, also $x + y$ eine Einheit. Dann sind $x' := \frac{x}{x+y}$ und $y' := \frac{y}{x+y}$ keine Einheiten, aber $x' + y' = 1$. Nach Voraussetzung müsste dann aber $1 - x' = y'$ eine Einheit sein, Wid.
c) $\Rightarrow$: Für $a, b \in R$ gilt $1_R = a * b \iff (1, 0, 0, \ldots) = (a_0 b_0, \ldots) \implies a_0 b_0 = 1 \implies a_0 \in K^\times$.
$\Leftarrow$: Sei $a = (a_0, a_1, \ldots) \in R$ und $a_0 \in K^\times$. Gesucht ist eine Folge $b_n \in K$ $(n \in \mathbb{N})$ mit

$$a * b = 1_R = (1, 0, 0, \ldots) \iff \bigwedge_{n \in \mathbb{N}} \sum_{k=0}^{n} a_k b_{n-k} = \delta_{0n}\,.$$

Da a_0 Einheit in K ist, kann man die Gleichung nach b_n auflösen und erhält so eine rekursive Definition für b_n $(n \in \mathbb{N})$ mit der gewünschten Eigenschaft $a * b = 1_R$. a ist also Einheit in R.
Die Nichteinheiten in R sind daher die Folgen a mit $a_0 = 0$. Diese sind offensichtlich additiv abgeschlossen und ein Ideal in R. Nach b) ist R also ein lokaler Ring.

Aufgabe 52. (s)
Es sei R ein kommutativer unitärer Ring. Eine Teilmenge S in R heißt *multiplikativ,* wenn sie multiplikativ abgeschlossen ist und die 1 enthält.

a) Zeigen Sie für ein echtes Ideal $\mathfrak{p} \lhd R$ die Äquivalenz

$$\mathfrak{p} \text{ Primideal} \iff R \setminus \mathfrak{p} \text{ multiplikativ}.$$

b) Sei nun R ein Integritätsbereich und $\mathfrak{p} \lhd R$ ein Primideal. Zeigen Sie

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

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

Lösung:
a) $\mathfrak{p} \neq R \iff 1 \notin \mathfrak{p} \iff 1 \in R \setminus \mathfrak{p}$. Daher gilt:

$$\begin{aligned} \mathfrak{p} \text{ Primideal} &\iff \textstyle\bigwedge_{a,b\in R} (ab \in \mathfrak{p} \implies a \in \mathfrak{p} \ \vee\ b \in \mathfrak{p}) \\ &\iff \textstyle\bigwedge_{a,b\in R} (a, b \notin \mathfrak{p} \implies ab \notin \mathfrak{p}) \\ &\iff R \setminus \mathfrak{p} \text{ multiplikativ.} \end{aligned}$$

b) $R_\mathfrak{p}$ ist ein Ring, denn für $r, r', s, s' \in R$, $s, s' \notin \mathfrak{p}$ gilt nach a) $ss' \notin \mathfrak{p}$ und daher

$$\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'} \in R_\mathfrak{p}, \quad \frac{r}{s} \pm \frac{r'}{s'} = \frac{rs' \pm r's}{ss'} \in R_\mathfrak{p}.$$

Weiter gilt

$$\frac{r}{s} \in (R_\mathfrak{p})^\times \iff \frac{s}{r} \in R_\mathfrak{p} \underset{(*)}{\iff} r \notin \mathfrak{p}.$$

$(*)$ $\Leftarrow$ ist klar. Für $\Rightarrow$ beachte man, dass ein Bruch natürlich seinen Nenner nicht eindeutig bestimmt, man also sorgfältig argumentieren muss: $s/r \in R_\mathfrak{p} \implies s/r = r'/s'$ mit $r' \in R, s' \notin \mathfrak{p}$, also $r'r = ss' \notin \mathfrak{p} \implies r \notin \mathfrak{p}$.
Damit folgt, dass die Menge der Nichteinheiten gerade das Ideal (!) $\mathfrak{p}.R_\mathfrak{p} = \{\frac{r}{s} \in R_\mathfrak{p} \mid r \in \mathfrak{p}, s \notin \mathfrak{p}\}$ ist und $R_\mathfrak{p}$ somit ein lokaler Ring.

Aufgabe 53. (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. 40)

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 $\mathbb{H}'$ die Quaternionengruppe Q_8 ist (vgl. Aufgabe 8).

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. 40).
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 $\mathbb{H}'^\times = \{\pm E, \pm S, \pm R, \pm T\}$ gleich der Quaternionengruppe Q_8 (siehe Aufgabe 8).

Aufgabe 54. (s)
Zeigen Sie als Anwendung des Zornschen Lemmas, dass *alle* (nicht nur endlich-dimensionale) Vektorräume über einem Körper K eine Basis besitzen.

Lösung:
Sei V ein K-Vektorraum und $\mathcal{M}$ die Menge der linear unabhängigen Teilmengen von V. $\mathcal{M}$ ist durch die Mengeninklusion eine geordnete Menge und nicht-leer ($\emptyset \in \mathcal{M}$). Sei nun $\mathcal{K} \subset \mathcal{M}$ eine Kette in $\mathcal{M}$, also eine totalgeordnete Menge von linear unabhängigen Teilmengen K_i ($i \in I$) von V. Eine solche Kette besitzt eine obere Schranke, nämlich: $B := \bigcup_{i \in I} K_i$. Wir zeigen, dass B eine linear unabhängige Teilmenge von V ist und damit $B \in \mathcal{M}$ eine obere Schranke für $\mathcal{K}$ ist. Wäre B linear abhängig, so gäbe es eine nicht-triviale 0-Darstellung als Linearkombination von

(endlich vielen) Vektoren $b_1, \ldots, b_n \in B = \bigcup_{i \in I} K_i$. Diese endlich vielen b_k liegen in endlich vielen Mengen $K_{i_k} \in \mathcal{K}$. Da die K_i eine Kette bilden, sind die endlich vielen Mengen K_{i_k} $(k = 1, \ldots, n)$ vergleichbar und es gibt ein K_i, das alle b_k enthält. Dann wäre aber K_i linear abhängig, im Widerspruch zu $K_i \in \mathcal{M}$.
Damit sind die Voraussetzungen des Zornschen Lemmas erfüllt und in der Menge $\mathcal{M}$ aller linear unabhängigen Teilmengen von V gibt es ein maximales Element B. Ein solches B ist Erzeugendensystem und damit Basis von V, denn andernfalls existierte ein $v \in V$, das keine Linearkombination von Elementen $b_k \in B$ wäre. Dann wäre aber $B' := B \cup \{v\}$ linear unabhängig, also $B' \in \mathcal{M}$ und B somit nicht maximal, Wid.

Algebra I
Übung 10

Aufgabe 55. (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. 46.

Aufgabe 56. (m)

a) Bestimmen Sie mit dem Euklidischen Algorithmus $\mathrm{ggT}(377, 233)$ und $\mathrm{ggT}(11050, 6916)$.

b) Für zwei natürliche Zahlen $a, b \in \mathbb{N}_+$ berechnen wir parallel drei Zahlenfolgen a_i, x_i, y_i durch

$$\begin{aligned} a_0 &= a\,,\ a_1 = b\,, & a_{i+1} &= a_{i-1} - q_i a_i \quad \text{mit } q_i = \lfloor \tfrac{a_{i-1}}{a_i} \rfloor \\ x_0 &= 1\,,\ x_1 = 0\,, & x_{i+1} &= x_{i-1} - q_i x_i\,, \\ y_0 &= 0\,,\ y_1 = 1\,, & y_{i+1} &= y_{i-1} - q_i y_i\,, \end{aligned}$$

Die Berechnung ist definiert, solange $a_i > 0$ ist. Sie endet, wenn $a_{i+1} = 0$ ist. Zeigen Sie, dass es ein solches i geben muss und dass dann gilt:

$$a_{i+1} = 0 \implies a_i = \mathrm{ggT}(a,b) = x_i a + y_i b\,.$$

[Tipp: Zeigen Sie $a_j = x_j a + y_j b$ für $0 \le j \le i$ und $d = a_i \mid a_j$ für $i+1 \ge j \ge 0$.]

c) Berechnen Sie mittels b) den $\mathrm{ggT}(119, 85)$ sowie seine Darstellung als ganzzahlige Linearkombination von 119 und 85.

Lösung:
a) $377 = 233 + 144\,,\ 233 = 144 + 89\,,\ 144 = 89 + 55\,,\ 89 = 55 + 34\,,\ 55 = 34 + 21\,,\ 34 = 21 + 13\,,\ 21 = 13{+}8\,,\ 13 = 8{+}5\,,\ 8 = 5{+}3\,,\ 5 = 3{+}2\,,\ 3 = 2{+}1\,,\ 2 = 2{\cdot}1{+}0 \implies \mathrm{ggT}(377, 233) = 1.$
Diese Kette hätte man früher abbrechen können, etwa $\mathrm{ggT}(377, 233) = \mathrm{ggT}(34, 21) = 1$, wobei für den letzten Schritt nicht der euklidische Algorithmus, sondern die Primzerlegung benutzt wird.
$11050 = 6916 + 4134\,,\ 6916 = 4134 + 2782\,,\ 4134 = 2782 + 1352\,,\ 2782 = 2 \cdot 1352 + 78\,,\ 1352 = 17 \cdot 78 + 26\,,\ 78 = 3 \cdot 26 + 0 \implies \mathrm{ggT}(11050, 6916) = 26.$
b) 1. Der Algorithmus endet: Nach Definition von q_i ist a_{i+1} der Rest bei Division von a_{i-1} durch a_i, also $0 \le a_{i+1} < a_i$. Da die a_i natürliche Zahlen sind, muss schließlich $a_{i+1} = 0$ erreicht werden.
2. $a_j = x_j a + y_j b$ für $j = 0, 1, \ldots, i$: Für $j = 0$ und $j = 1$ ist die Behauptung unmittelbar aus der

Definition ablesbar. Und aufgrund der gleichartigen Definition von a_{j+1}, x_{j+1} und y_{j+1} erhält man induktiv die Behauptung für alle $j \leq i$.
3. $d = a_i$ ist gemeinsamer Teiler von a und b:
Wir zeigen induktiv $d \mid a_j$ für alle $j = i+1, i, \ldots, 1, 0$, insbesondere also $d \mid a_0 = a$ und $d \mid a_1 = b$.
Der Induktionsanfang ist klar: $d \mid 0 = a_{i+1}$.
Sei nun d ein Teiler aller a_k mit $k \geq j$. Dann ist d auch ein Teiler von $a_{j+1} + q_j a_j = a_{j-1}$. Damit ist auch der Induktionsschritt bewiesen.
4. $d = \mathrm{ggT}(a, b)$:
Nach 3. ist d ein gemeinsamer Teiler von a und b. Ist $d' \in \mathbb{N}$ irgendein weiterer gemeinsamer Teiler von a und b, so ist d' nach 2. ein Teiler aller a_j, insbesondere auch ein Teiler von $a_i = d$. Damit ist d der größte gemeinsame Teiler von a und b.
c)

i	0	1	2	3	4
a	119	85	34	17	0
x	1	0	1	-2	
y	0	1	-1	3	
q		1	2	2	

$\Longrightarrow\ 17 = \mathrm{ggT}(119, 85) = -2 \cdot 119 + 3 \cdot 85\,.$

Aufgabe 57. (m)
Sei G eine endliche abelsche Gruppe. Zeigen Sie:

a) $\displaystyle\prod_{a \in G} a = \prod_{\substack{a \in G \\ a^2 = e}} a.$

b) Folgern Sie den Satz von Wilson: $(p-1)! \equiv -1 \bmod p$ für jede Primzahl p.

Lösung:
a) G ist abelsch, so dass die Produkte (von der Reihenfolge unabhängig) wohldefiniert sind. Es ist $\displaystyle\prod_{a \in G} a = \prod_{a^2 = e} a \cdot \prod_{a \neq a^{-1}} a$. In dem letzten Produkt $\displaystyle\prod_{a \neq a^{-1}} a$ kann man die Faktoren umsortieren und jeweils Paare a, a^{-1} als Faktoren zusammenfassen, also ist dieses Produkt gleich e und die Behauptung bewiesen.
b) Mit $G = \mathbb{F}_p^\times$ gilt $(p-1)! + \mathrm{mod} p\mathbb{Z} = \prod_{a \in G} a$ und da $\mathbb{F}_p$ ein Körper ist, gilt $a^2 = e \iff a = \pm 1$ für $a \in G$. Also folgt nach a) $(p-1)! \equiv (+1) \cdot (-1) = -1 \bmod p$.

Aufgabe 58. (s)
Zeigen Sie durch Rechnungen in Restklassenringen von $\mathbb{Z}$:

a) Eine natürliche Zahl n ist genau dann durch 9 teilbar, wenn ihre Quersumme (=Summe der Ziffern der Dezimaldarstellung von n) durch 9 teilbar ist.

b) Formulieren und beweisen Sie eine *Elferprobe.*

c) Man bestimme den Rest von $(123578^{51} + 283679^5)^{154}$ bei Division durch 143.

[Tipp: Lösen Sie die Aufgabe zunächst für die Primteiler von 143 und beachten Sie den Chinesischen Restsatz.]

Lösung:
Sei $a = \sum_k a_k 10^k$ die Dezimaldarstellung von a, also $a_k \in \mathbb{N}$, $0 \leq a_k \leq 9$ die Folge der Dezimalziffern von a.
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 genau dann durch 9 teilbar, wenn die Quersumme es ist.

b) 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.
c) Sei A die vorgegebene Zahl; gesucht ist $a \in \mathbb{Z}$, $0 \le a < 143$ mit $a \equiv A \bmod 143$. Es ist $143 = 11 \cdot 13$ und wegen der Teilerfremdheit von 11 und 13 gilt daher

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

Wir berechnen daher zunächst A modulo beider 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:

$$\begin{aligned} \mathrm{mod}11: &\quad A = (123578^{51} + 283679^5)^{154} \equiv (4^1 + 0)^4 \equiv 16 \cdot 16 \equiv 5 \cdot 5 \equiv 3\,,\\ \mathrm{mod}13: &\quad A = (123578^{51} + 283679^5)^{154} \equiv (0 + 6^5)^{10} \equiv 6^{50} \equiv 6^2 \equiv -3 \end{aligned}$$

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 $a = 33 + 3 = 39 - 3$.

Aufgabe 59. (s)
Es seien $a, b, c \in \mathbb{Z}$ und a, b teilerfremd. Es sei W die Lösungsmenge der linearen *diophantischen* Gleichung $ax + by = c$, d. h. die Menge der ganzzahligen Lösungen dieser Gleichung. (Allgemein sind diophantische Gleichungen Polynomgleichungen mit ganzzahligen Koeffizienten, deren *ganzzahlige* Lösungen bestimmt werden sollen.) Zeigen Sie:

a) W ist nicht leer. Geben Sie ein Verfahren zur Bestimmung einer Lösung $(x_0, y_0) \in W$ an.

b) Ist $(x_0, y_0) \in W$, so gilt $W = \{(x_0 + nb, y_0 - na) \mid n \in \mathbb{Z}\}$.

c) Lösen Sie die diophantische Gleichung $15x + 8y = 5$.

Lösung:
a) Wegen $\mathrm{ggT}(a, b) = 1$ kann man mit dem euklidischen Algorithmus $x, y \in \mathbb{Z}$ bestimmen, mit $xa + yb = 1$. Also ist $(x_0, y_0) = (cx, cy)$ eine ganzzahligen Lösung der Gleichung $ax + by = c$.
b) Sei $(x, y) \in W$, also $ax + by = c = ax_0 + by_0 \iff a(x - x_0) = -b(y - y_0)$. Da a, b teilerfremd sind, folgt $a \mid y - y_0$ und $b \mid x - x_0$, also existieren $n, m \in \mathbb{Z}$ mit $y - y_0 = am\,,\ x - x_0 = bn$. Wegen $abn = a(x - x_0) = -b(y - y_0) = -bam$ muss $m = -n$ sein und es folgt $x = x_0 + bn$, $y = y_0 - an$.
c) 15 und 8 sind teilerfremd und es gilt $1 = -15 + 2 \cdot 8$, also $5 = -5 \cdot 15 + 10 \cdot 8$. Damit ist $(-5, 10) \in W$ und $W = \{(-5 + 8n, 10 - 15n) \mid n \in \mathbb{Z}\} = \{\ldots, (-13, 25), (-5, 10), (3, -5), (11, -20), \ldots\}$ die gesuchte Lösungsmenge.

Aufgabe 60. (s)
Seien $r \in \mathbb{N}_+$, $n_i \in \mathbb{N}$ $(i = 1, \dots r)$ teilerfremd und $N := \prod_{i=1}^{r} n_i$ sowie $N_i := \frac{N}{n_i}$. Zeigen Sie:

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

b) Mit den N_i' wie in a) gilt für beliebig vorgegebene $a_1, \dots, a_r \in \mathbb{Z}$:

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

Die Lösungsmenge L der *simultanen Kongruenzen* $x \equiv a_i \bmod n_i$ $(i = 1, \dots, r)$ modulo teilerfremder Moduln n_i ist genau die volle Restklasse $a + N\mathbb{Z}$ modulo N des Elementes $a := \sum_{i=1}^{r} N_i N_i' a_i$.

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

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

Lösung:
a) 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. 49): $N_i N_i' \equiv 1 \bmod n_i$, wie behauptet.
b) $\Leftarrow$: Wegen $N = \prod_i n_i$ gilt

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

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

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

c) 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 $N = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$

$$a = \sum_i N_i N_i' a_i = 385 \cdot 1 \cdot 2 + 231 \cdot 1 \cdot 3 + 165 \cdot 2 \cdot 4 + 105 \cdot 2 \cdot 5 = 3833 \equiv 368 \bmod N\,.$$

Aufgabe 61. (s)
Sei $d \in \mathbb{Z}_+$ und $R := \mathbb{Z}[i\sqrt{d}]$. Wir definieren die sog. *Normabbildung* $\mathcal{N} : R \to \mathbb{N}$, $\alpha \mapsto \alpha\bar{\alpha} = |\alpha|^2$.

a) Zeigen Sie für $\alpha, \beta \in R$:
   (1) $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha) \cdot \mathcal{N}(\beta)$
   (2) $\alpha \mid \beta$ in R $\implies$ $\mathcal{N}(\alpha) \mid \mathcal{N}(\beta)$ in $\mathbb{Z}$.
   (3) $\alpha \in R^\times \iff \mathcal{N}(\alpha) = 1$.
   (4) $(\mathbb{Z}[i\sqrt{d}])^\times = \{\pm 1\}$ für $d \geq 2$ und $(\mathbb{Z}[i])^\times = \{\pm 1, \pm i\}$.
   (5) Ist α Teiler von β in R, so gilt: α, β assoziiert in $R \iff \mathcal{N}(\alpha) = \mathcal{N}(\beta)$.

b) Bestimmen Sie für $\alpha = 21 + 63i$, $\beta = 110i$ eine Zerlegung in Primelemente von $\mathbb{Z}[i]$ und einen ggT.

c) Zeigen Sie: $R = \mathbb{Z}[i\sqrt{6}]$ ist nicht faktoriell, da 10 in R zwei wesentlich verschiedene Zerlegungen in unzerlegbare Elemente hat.

Lösung:
(1) ist klar. (2) klar nach (1).
(3): $\alpha\beta = 1 \implies \mathcal{N}(\alpha)\mathcal{N}(\beta) = 1 \implies \mathcal{N}(\alpha) = \mathcal{N}(\beta) = 1$, da alle Normen in $\mathbb{N}$ liegen. Und umgekehrt $1 = \mathcal{N}(\alpha) = \alpha\bar{\alpha} \implies \alpha \in R^\times$, denn $\bar{\alpha} \in R$
(4): Sei $R = \mathbb{Z}[i\sqrt{d}]$. Für $d \geq 2$ und $a, b \in \mathbb{Z}$ gilt:

$$z := a + b \cdot i\sqrt{d} \in R^\times \iff \mathcal{N}(a + b \cdot i\sqrt{d}) = a^2 + db^2 = 1 \underset{d \geq 2}{\iff} a^2 = 1 \wedge b = 0 \iff z = \pm 1\,.$$

Für $d = 1$ folgt entsprechend $z \in R^\times \iff a^2 + b^2 = 1 \iff a^2 = 1, b = 0 \vee a = 0, b^2 = 1 \iff z = \pm 1, \pm i$.
(5): Ist $\alpha = \beta\varepsilon$ mit $\varepsilon \in R^\times$, so folgt nach (3) $\mathcal{N}(\alpha) = \mathcal{N}(\beta) \cdot 1$. Umgekehrt gilt für $\beta = \gamma\alpha$ mit $\gamma \in R$ und $\alpha \neq 0$: $\mathcal{N}(\alpha) = \mathcal{N}(\beta) \iff \alpha\bar{\alpha} = \beta\bar{\beta} = \gamma\alpha \cdot \bar{\gamma}\bar{\alpha} \iff \gamma\bar{\gamma} = 1 \underset{(3)}{\iff} \gamma \in R^\times$.
b) $R = \mathbb{Z}[i]$ ist euklidisch (Beispiele II.2.10 2)), also Hauptidealring und faktoriell. Unzerlegbare Elemente sind daher Primelemente.
Es ist $\alpha = 21 + 63i = 3 \cdot 7 \cdot (1 + 3i)$. Wir untersuchen die auftretenden Faktoren 3, 7, $1 + 3i$ auf mögliche *echte* Teiler, also Nichteinheiten und nicht Assoziierte. Gemäß a) kommen dafür nur Teiler $z = a + bi$ in Frage, deren Norm $\mathcal{N}(z) = a^2 + b^2$ *echter* (!) Teiler von $\mathcal{N}(3) = 3^2$, $\mathcal{N}(7) = 7^2$ oder $\mathcal{N}(1 + 3i) = 10$ ist.
1. $N := a^2 + b^2 = 3$: Dies ist unlösbar in $\mathbb{N}$ und damit ist 3 unzerlegbar in R.
2. Genauso: 7 ist unzerlegbar.
3a. $N = a^2 + b^2 = 2$: $a^2 + b^2 = 2 \iff a^2 = b^2 = 1 \iff z = z = \pm 1 \pm i$. Diese 4 Elemente sind assoziiert zu $1 + i$ und $1 + i$ ist Teiler von $1 + 3i = (1 + i)(2 + i)$.
3b. $N = a^2 + b^2 = 5$: $a^2 + b^2 = 5 \iff a^2 = 1, b^2 = 4 \vee a^2 = 4, b^2 = 1 \iff z = \pm(1 \pm 2i) \vee z = \pm(2 \pm i)$. Von diesen 8 möglichen Teilern sind aber nur die 4 Assoziierten von $2 + i$ (vgl. 3a.) Teiler von $1 + 3i$.
$1 + i$ und $2 + i$ sind unzerlegbar, weil ihre Normen Primzahlen sind, und wir erhalten für $21 + 63i$ in R die Primzerlegung

$$21 + 63i = 3 \cdot 7 \cdot (1 + i) \cdot (2 + i)\,.$$

Es ist $\beta = 110i = 2 \cdot 5 \cdot 11 \cdot i$: i ist Einheit und 11 ist unzerlegbar ($a^2 + b^2 = 11$ in $\mathbb{N}$ unlösbar, wie oben für 3 und 7).
$a^2 + b^2 = 2$ hat die in 3a. bestimmten 4 Lösungen, die in R zur Zerlegung $2 = (1 + i)(1 - i)$ führen. Die Faktoren $1 \pm i$ haben Norm 2 und sind unzerlegbar.
$a^2 + b^2 = 5$ hat die in 3b. bestimmten 8 Lösungen, die in R zu folgender Zerlegung führen: $5 = (1 + 2i)(1 - 2i)$, wobei die einzelnen Faktoren wieder unzerlegbar sind.

Damit erhalten wir in R für $110i$ die folgende Primzerlegung

$$110i = (1+i)\cdot(1-i)\cdot 11\cdot(1+2i)\cdot i(1-2i)\,.$$

Mit $i(1-2i) = 2+i$ entnimmt man aus beiden Primzerlegungen nun leicht einen ggT:

$$\mathrm{ggT}(\alpha,\beta) = (1+i)(2+i) = (1+3i)\,.$$

Man beachte, dass Primfaktoren und ggT nur eindeutig sind bis auf Assoziiertheit, also bis auf Multiplikation mit einer der 4 Einheiten ± 1 und $\pm i$ in R.
c) Sei nun $R = \mathbb{Z}[i\sqrt{6}]$. Gesucht sind echte Teiler $z = a + bi\sqrt{6}$ von 10 in R, also echte Teiler $\mathcal{N}(z) = a^2 + 6b^2$ von $2^2 \cdot 5^2$. Die Teiler 2 und 5 mit den Normen 2^2 bzw. 5^2 sind natürlich klar. Wir untersuchen $a^2 + 6b^2 = 10$: Dann folgt $a^2 = 4, b^2 = 1$, also $z = \pm 2 \pm i\sqrt{6}$. Dies führt zur Zerlegung $10 = (2 + i\sqrt{6})(2 - i\sqrt{6})$. Die so gefundenen vier echten Teiler von 10 in R sind alle unzerlegbar, denn ihre Normen 4, 25 und 10 haben nur die echten Teiler 2 und 5 und diese sind keine Normen $a^2 + 6b^2$. Außerdem sind diese 4 Faktoren 2, 5, $2 \pm i\sqrt{6}$ nicht zueinander assoziiert (nur ± 1 sind Einheiten in R gemäß a)(4)).

Algebra I
Übung 11

Aufgabe 62. (m)
Sei $G = \langle\sigma\rangle$ zyklisch von der Ordnung n und $k \in \mathbb{Z}$. Zeigen Sie:

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

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

c) $\operatorname{Aut} G \simeq \mathcal{P}(n)$ prime Restklassengruppe modulo n

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

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

Lösung:
a) folgt aus b). Hier ein Beweis als Hinführung zu b):

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

b) Sei $d = \operatorname{ggT}(n,k)$ und $dn' = n$, $dk' = k$, also n', k' teilerfremd. Dann gilt für 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.
c): $f \in \operatorname{Aut} G \implies f(\sigma) =: \sigma^k$ erzeugt $f(G) = G$, also ist nach a) $\bar{k} \in \mathcal{P}(n)$. 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 a) $f(\sigma) = \sigma^k$ 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 $\Phi(f) = \bar{k}$.
d) Für $\sigma = (\sigma_1, \sigma_2) \in G_1 \times G_2$ gilt $\operatorname{ord}(\sigma_1, \sigma_2) = \operatorname{kgV}(\operatorname{ord}\sigma_1, \operatorname{ord}\sigma_2)$, 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 $\operatorname{kgV}(n_1, n_2)$. 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

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

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

Aufgabe 63. (m)
Bestimmen Sie den ggT der Polynome $f = X^6 + \bar{2}X^5 + \bar{3}X^4 + \bar{5}X^3 + X^2 + \bar{3}X + \bar{6} \in \mathbb{F}_7[X]$ und $g = X^5 + \bar{5}X^3 + X^2 + \bar{5} \in \mathbb{F}_7[X]$.

Lösung:
Wir verwenden den euklidischen Algorithmus und führen sukzessive Polynomdivision durch. Dabei werden die Divisor-Polynome in $\mathbb{F}_7[X]$ jeweils normiert, wodurch sich die die Teilbarkeit natürlich nicht ändert. Dadurch kann man die Polynomdivision per Hand über $\mathbb{Z}$ durchführen und muss nur danach den Rest modulo 7 reduzieren. Alle folgenden Gleichungen gelten über $\mathbb{F}_7$. Es sei $f_0 := f$ und $f_1 := g$.

$$\begin{array}{lcl}
r_2 := f_0 - (X+2)f_1 & = & -2X^4 - 6X^3 - X^2 - 2X - 4 \\
f_2 := 3r_2 & = & X^4 + 3X^3 - 3X^2 + X + 2 \\
\hline
r_3 := g - (X-3)f_2 & = & 3X^3 - 2X^2 + X + 4 \\
f_3 := -2r_3 & = & X^3 - 3X^2 - 2X - 1 \\
\hline
r_4 := f_2 - (X-1)f_3 & = & 3X^2 + 1 \\
f_4 := -2r_4 & = & X^2 - 2 \\
\hline
r_5 := f_3 - (X-3)f_4 & = & 0
\end{array}$$

Mit $r_5 = 0$ erhalten wir $\mathrm{ggT}(f, g) = f_4 = X^2 - \bar{2} \in \mathbb{F}_7[X]$.
Eine erste *Kontrolle* dieser durchaus fehleranfälligen Rechnung erhält man wie folgt: $X^2 - 2$ hat über $\mathbb{F}_7$ die Nullstellen ± 3, diese müssen also gemeinsame Nullstellen von f, g sein (und sind es auch). Damit ist unabhängig von obiger Rechnung $X^2 - 2$ ein gemeinsamer Teiler von f, g.
Dass er tatsächlich der ggT ist, erhält man aus seiner Darstellung als Linearkombination, die man aus obigen Gleichungen bestimmen kann:

$$\begin{array}{rcl}
f_4 & = & -2(f_2 - (X-1)f_3) = -2f_2 + 2(X-1)f_3 \\
& = & -2f_2 + 2(X-1)(-2)(g - (X-3)f_2) \\
& = & g \cdot (-4(X-1)) + (-2 + 4(X-1)(X-3)) \cdot f_2 \\
& = & g \cdot (-4X + 4) + (4X^2 - 2X + 3) \cdot 3(f - (X+2)g) \\
& = & g(-4X + 4 - 3(4X^2 - 2X + 3)(X+2)) + 3(4X^2 - 2X + 3)f \\
& = & (-2X^2 + X + 2)f + (2X^3 + 3X^2 - X)g
\end{array}$$

Aufgabe 64. (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. 51) 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) Wir setzen $(b_1, \ldots, b_n) := (a_1, \ldots, a_n) \cdot A$.

'$\Rightarrow$': Ist $(b_1, \ldots, b_n)$ 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 $\frac{1}{\det A} A^{\mathrm{ad}} \in M_n(R)$.
'$\Leftarrow$': 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

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

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

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 65. (s)
Sei $(A,+)$ eine endliche abelsche Gruppe und für $n \in \mathbb{N}_+$ sei $A(n) := \{a \in A \mid na = 0\}$. Bestätigen Sie, dass $A(n)$ eine Untergruppe von A ist. Zeigen Sie:

a) Sei p ein Primteiler von $\#A$ und $\nu \in \mathbb{N}_+$ maximal mit $p^\nu \mid \#A$. Dann ist $A(p^\nu)$ die(!) p-Sylowgruppe von A.

b) Sei $\#A = n \cdot m$ mit teilerfremden $n, m \in \mathbb{N}$. Dann gilt $A = A(n) \oplus A(m)$.

c) Sei $\#A = \prod_{i=1}^{r} p_i^{\nu_i}$ mit verschiedenen Primzahlen p_i. Dann gilt: $A = \bigoplus_{i=1}^{r} A(p_i^{\nu_i})$, d. h. endliche abelsche Gruppen sind direkte Summe ihrer Sylowgruppen.

Lösung:
Da A abelsch ist, gilt $na = 0 = nb \implies n(a-b) = na - nb = 0$, also $A(n) \leq A$.
a) Da A abelsch ist, sind die Sylowuntergruppen Normalteiler und daher eindeutig. Sei A_p die p-Sylowgruppe von A, also $\#A_p = p^\nu$, dann gilt für alle $a \in A_p$ $p^\nu a = \#A_p \cdot a = 0$ und somit $A_p \subset A(p^\nu)$. Umgekehrt gilt für jedes $a \in A(p^\nu)$ $p^\nu a = 0$, so dass $\#\langle a\rangle = \operatorname{ord} a$ eine p-Potenz und $\langle a\rangle$ eine p-Untergruppe von A ist. Diese muss in der (einzigen) p-Sylowgruppe A_p liegen, also: $A(p^\nu) \subset A_p$.
b) $a \in A(n) \cap A(m) \implies na = 0 = ma \implies \operatorname{ord} a \mid n, m \implies \operatorname{ord} a \mid \operatorname{ggT}(n,m) = 1 \implies a = 0$. Damit haben $A(n)$ und $A(m)$ trivialen Schnitt.
Für alle $a \in A$ gilt $nma = \#A \cdot a = 0$. Wegen $1 = \operatorname{ggT}(n,m)$ gibt es eine Darstellung $1 = xn + ym$ mit $x, y \in \mathbb{Z}$. Daraus erhalten wir für alle $a \in A$

$$a = 1 \cdot a = xna + yma =: a_m + a_n \quad \text{mit} \quad a_m \in A(m)\,,\ a_n \in A(n)\,,$$

denn $ma_m = xnma = 0$ und $na_n = ynma = 0$. Damit ist $A = A(n) \oplus A(m)$.
c) folgt induktiv aus b).

Aufgabe 66. (s)
Sei p eine Primzahl und $r, s \in \mathbb{N}$. Ist A eine endliche abelsche p-Gruppe mit

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

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

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

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 $\mathbb{Z}/p^0\mathbb{Z} = 0$)

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

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 $1 \leq i < a = b$. Nach Induktionsvoraussetzung folgt dann schließlich

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

Aufgabe 67. (s)

a) Sei R ein faktorieller Ring, K sein Quotientenkörper und $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ein *normiertes* Polynom vom Grad $n \geq 1$. Zeigen Sie:

Ist $\alpha \in K$ eine Nullstelle von f, so gilt $\alpha \in R$ und $\alpha \mid a_0$.

b) Bestimmen Sie alle rationalen Nullstellen der Polynome $f = X^3 + 2X^2 - X - 2 \in \mathbb{Z}[X]$ und $g = X^n - p$, $n \geq 2$, p Primzahl. Was folgern Sie für $\sqrt[n]{p}$?

c) Formulieren Sie ein (notwendiges und hinreichendes) Irreduzibilitätskriterium für Polynome vom Grade ≤ 3 über Körpern.

Lösung:
a) Sei $\alpha = \frac{x}{y}$ mit $x, y \in R$ teilerfremd. Dann gilt

$$0 = f(\frac{x}{y}) \implies 0 = y^n f(\frac{x}{y}) = \sum_{i=0}^{n-1} a_i x^i y^{n-i} + x^n \implies y \mid \sum_{i=0}^{n-1} a_i x^i y^{n-i} = -x^n\,.$$

Wäre $\alpha \notin R$, so hätte y einen Primteiler und es folgte $p \mid y \mid x^n \implies p \mid x$, im Widerspruch zur Teilerfremdheit von x, y. Also ist $\alpha \in R$ und Polynomdivision von f durch $X - \alpha \in R[X]$ (normiert!) ergibt $f(X) = q(X) \cdot (X - \alpha)$ mit $q(X) \in R[X]$ und damit $a_0 = f(0) = q(0) \cdot (-\alpha)$, also $\alpha \mid a_0$.
b) Als rationale Nullstellen von f bzw. g kommen nach a) nur Teiler des absoluten Gliedes in Frage.
Bei f sind dies $\pm 1, \pm 2$ und durch Einsetzen findet man als rationale Nullstellen ± 1 und 2.
Bei g sind die einzig möglichen rationalen Nullstellen ± 1 und $\pm p$. Für $n \geq 2$ ist keine dieser Möglichkeiten tatsächlich Nullstelle: $X^n - p$ hat keine rationalen Nullstellen. Dies bedeutet $\sqrt[n]{p}$ ist irrational für $n \geq 2$.
c) Ein Polynom vom Grad 2 oder 3 ist genau dann irreduzibel, wenn es keine Nullstelle hat.

Algebra I
Übung 12

Aufgabe 68. (s)

a) (Irreduzibilitätskriterium von Eisenstein)

Sei R ein faktorieller Ring und $f = \sum_i a_i X^i \in R[X]$ vom Grade $n \geq 1$. Für ein Primelement p von R gelte

(1) $p \nmid a_n$, (2) $p \mid a_i$ für $0 \leq i < n$, (3) $p^2 \nmid a_0$.

Zeigen Sie: f ist irreduzibel in $R[X]$.

[Tipp: Betrachten Sie für eine Zerlegung $f = gh$ mit $g = \sum_i b_i X^i \in R[X]$, $h = \sum_j c_j X^j \in R[X]$ die minimalen Indizes ν mit $p \nmid b_\nu$ bzw. μ mit $p \nmid c_\mu$. Zeigen Sie $\mu = 0$, $\nu \geq 1$ (oder umgekehrt) und untersuchen Sie dann a_ν.]

b) Sei R ein kommutativer unitärer Ring, $u \in R^\times$, $a \in R$. Zeigen Sie für $f \in R[X]$

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

c) Sei $f = \sum_i a_i X^i \in \mathbb{Z}[X]$ ein Polynom vom Grade n und p eine Primzahl mit $p \nmid a_n$. Es sei $\bar{f} \in \mathbb{F}_p[X]$ das Restklassenpolynom von f modulo p. Zeigen Sie:

$$\bar{f} \in \mathbb{F}_p[X] \text{ irreduzibel} \implies f \in \mathbb{Z}[X] \text{ irreduzibel}\,.$$

d) Zeigen Sie, dass die folgenden Polynome in $\mathbb{Z}[X]$ irreduzibel sind:

$f(X) = 93X^4 - 28X^3 - 63X^2 + 49X + 14$,

$g(X) = X^4 + 1$ und $h(X) = 5X^5 - 8X^4 - 2X^3 + 3X^2 + 12X + 11$.

Lösung:

a) Sei $f = gh$ wie im Tipp. Wegen $p \nmid a_n$ können nicht alle Koeffizienten von g bzw. von h durch p teilbar sein, ν und μ existieren wie definiert. Wegen $p \mid a_0 = b_0 c_0$ und $p^2 \nmid b_0 c_0$, gilt o. E. $p \mid b_0$ und $p \nmid c_0$ und damit $\nu \geq 1$. Dann gilt

$$a_\nu = \sum_{i+j=\nu} b_i c_j = \sum_{i<\nu} b_i c_{\nu-i} + b_\nu c_0\,.$$

Der Summenterm ist wegen der Minimalität von ν durch p teilbar, also folgt $a_\nu \equiv b_\nu c_0 \bmod p$. Wegen $p \nmid b_\nu$ und $p \nmid c_0$ folgt $p \nmid a_\nu$, also $\nu = n$. Damit hat g den Grad n und h ist konstant, f ist somit irreduzibel über R.

b) $f(X) = g(X)h(X) \implies f(uX + a) = g(uX + a)h(uX + a)$ und, da sich bei der linearen Substitution $uX + a$ die Grade nicht ändern, folgt aus der Reduzibilität von f die von $f(uX + a)$. Umgekehrt schließt man genauso mit der inversen linearen Substitution $u^{-1}X - u^{-1}a \in R[X]$.

c) Wir schließen indirekt. Eine Zerlegung $f = gh$ in Faktoren kleineren Grades aus $\mathbb{Z}[X]$ ergibt eine Zerlegung $\bar{f} = \bar{g}\bar{h}$ in $\mathbb{F}_p[X]$, wobei sich wegen $p \nmid a_n$, also $\bar{a}_n \neq 0$ die Grade nicht ändern: $\bar{f}$ ist reduzibel.

d) f ist ein Eisensteinpolynom für die Primzahl 7, also nach a) irreduzibel in $\mathbb{Z}[X]$.
$g(X + 1) = X^4 + 4X^3 + 6X^2 + 4X + 2$ ist ein 2-Eisensteinpolynom, also irreduzibel in $\mathbb{Z}[X]$. Gemäß b) ist dann auch $g(X)$ irreduzibel.
Sei $p = 2$ und $\bar{f}$ die Reduktion von f modulo 2, also $\bar{f} = X^5 + X^2 + 1 \in \mathbb{F}_2[X]$. $\bar{f}$ hat keine Nullstelle in $\mathbb{F}_2$, wenn also $\bar{f}$ reduzibel ist, muss es in einen quadratischen und einen kubischen Faktor zerfallen. $\bar{f}$ muss also in $\mathbb{F}_2[X]$ einen quadratischen Faktor ohne Nullstelle haben. Ein quadratischen Polynom $q(X) := X^2 + aX + b \in \mathbb{F}_2[X]$ hat genau dann keine Nullstelle in $\mathbb{F}_2$, wenn $a = b = 1$ ist. Dieses quadratische Polynom $X^2 + X + 1$ ist aber kein Teiler von $\bar{f} = X^5 + X^2 + 1$ in $\mathbb{F}_2[X]$, denn Polynomdivision ergibt in $\mathbb{F}_2[X]$ $\bar{f} = (X^2 + X + 1) \cdot (X^3 + X^2) + 1$. Folglich ist $\bar{f}$ irreduzibel in $\mathbb{F}_2[X]$ und nach c) dann auch f in $\mathbb{Z}[X]$.

Aufgabe 69. (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.

d) Beweisen Sie den *Satz von Gauß*:

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

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 71 b)). 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_1d_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.
d) Wir zeigen zuerst, dass unzerlegbare Elemente in $R[X]$ prim sind. Für Elemente aus R ist dies nach Voraussetzung richtig. Sei $f \in R[X] \setminus R$ unzerlegbar. Nach Teil 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. 57). Da $K[X]$ faktoriell ist (Vorlesung Satz II.3.6, S. 57), 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 $K[X]$:

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

Da R faktoriell ist, sind o. E. α, β teilerfremd. Da nach Teil 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 Teil c) unzerlegbar in $R[X]$ und nach 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 70. (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:

$$R[X]/(X-a)R[X] \simeq R\,.$$

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

$$R[X]/(X - a)R[X] = R[X]/\operatorname{Ke} E_a \xrightarrow{\sim} \operatorname{Im} E_a = R\,.$$

Aufgabe 71. (m)
R sei ein kommutativer unitärer Ring und $\deg : R[X] \setminus \{0\} \to \mathbb{N}$ die Gradfunktion. Zeigen Sie:

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) R Körper $\iff$ $R[X]$ Hauptidealring.

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 $\rho > m+n$, also $\deg(fg) \leq m+n$, und für nullteilerfreies R gilt $c_{m+n} = a_m b_n \neq 0$, also $\deg(fg) = m+n$, und der führende Koeffizient von fg ist das Produkt der führenden Koeffizienten von f und von g.
b) Es genügt der Beweis für $n = 1$, die allgemeine Behauptung folgt daraus induktiv mittels der vorangehenden Aufgabe 70 a).
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 ' $\Longrightarrow$ ' gezeigt ist; '$\Longleftarrow$' ist klar wegen $R \leq R[X]$.
c) '$\Rightarrow$' ist klar nach Satz II.3.6. '$\Leftarrow$': Als Hauptidealring ist $R[X]$ und damit auch R ein Integritätsbereich. Sei $0 \neq a \in R$. Das Ideal $\mathfrak{a} := aR[X] + XR[X] = \{f \in R[X] \mid a \mid f(0)\} \lhd R[X]$ ist nach Voraussetzung Hauptideal, also $\mathfrak{a} = g \cdot R[X]$. Wegen $a \in \mathfrak{a}$ muss aus Gradgründen $g = b \in R$ sein und es gilt $a \mid b$. Wegen $X \in \mathfrak{a}$ gibt es ein $h \in R[X]$ mit $X = b \cdot h$, also $1 = b \cdot d$ für den führenden Koeffizienten d von h. Damit ist b eine Einheit und wegen $a \mid b$ folgt auch $a \in R^\times$: $R \setminus \{0\} \subset R^\times$, R ist ein Körper.

Aufgabe 72. (s)
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 ist die Potenzierung mit p ein Körpermonomorphismus $\varphi : k \to k$, $a \mapsto a^p$.

c) Ist k ein endlicher Körper, so ist φ ein Automorphismus von k. Allgemein gilt dies nicht.

Lösung:
a) Für $1 \leq i \leq p$ 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) Bzgl. der Multiplikation ist φ in jedem kommutativen Ring ein Homomorphismus. Nun zur Addition: Wegen $\operatorname{char} k = p$ gilt $p.1_k = 0$ und daher $p.c = 0$ für alle $c \in k$. Also folgt

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

Damit ist φ ein additiver Homomorphismus. Als Körperhomomorphismus ist φ ein Monomorphismus.
c) Ist k endlich, so muss φ als injektive Selbstabbildung auch surjektiv sein. Als Gegenbeispiel für unendliches k betrachten wir den Quotientenkörper des Polynomrings $\mathbb{F}_p[X]$, den rationalen Funktionenkörper $k := \mathbb{F}_p(X)$ in einer Unbestimmten. $X \in k$ kann keine p-te Potenz sein, denn aus Gradgründen kann es keine Polynome $f, g \in \mathbb{F}_p[X]$ geben mit

$$X = (\frac{f}{g})^p \iff Xg^p = f^p .$$

Aufgabe 73. (s)

a) Sei $K|k$ eine Körpererweiterung, $f = \sum_i a_i X^i \in k[X]$ ein Polynom vom Grade $n \geq 1$ und $\alpha \in K$ eine Wurzel von f. Zeigen Sie: $1, \alpha, \ldots, \alpha^{n-1}$ ist ein k-Erzeugendensystem von $k[\alpha]$.

b) m und n seien verschiedene *quadratfreie* ganze Zahlen $\neq 0$, das heißt m und n seien nicht durch Quadrate ganzer Zahlen > 1 teilbar. Zeigen Sie $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n})$ und bestimmen Sie den Körpergrad über $\mathbb{Q}$.

c) Es sei $k = \mathbb{Q}(\sqrt[4]{2}, i) \subset \mathbb{C}$. Bestimmen Sie den Grad $(k : \mathbb{Q})$.

Lösung:
a) Es ist

$$k[\alpha] = \operatorname{Im} E_\alpha = \{h(\alpha) \mid h \in K[X]\} = \{\sum_{\nu=0}^{m} c_\nu \alpha^\nu \mid m \in \mathbb{N}\,,\ c_\nu \in k\}$$

und daher hat $k[\alpha]$ die Potenzen α^ν $(\nu \in \mathbb{N})$ als k-Erzeugendensystem. Wir zeigen, dass bereits $B := \{\alpha^\nu \mid 0 \le \nu < m\}$ ein Erzeugendensystem ist, denn es gilt:

$$\alpha^\nu \in \langle 1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\rangle_k \quad \text{für alle } \nu \in \mathbb{N}\,.$$

Für $0 \le \nu \le n-1$ ist nichts zu zeigen. Sei nun $l \ge n$ und es gelte die Behauptung für alle $\nu < l$. Gemäß Voraussetzung gilt

$$\begin{aligned} 0 = f(\alpha) &= \sum_{\nu=0}^{n-1} a_\nu \alpha^\nu + a_n \alpha^n \implies \alpha^n = -a_n^{-1} \sum_{\nu=0}^{n-1} a_\nu \alpha^\nu \\ \implies \alpha^l &= -a_n^{-1} \sum_{\nu=0}^{n-1} a_\nu \alpha^{l-n+\nu} \underset{\text{Ind.Vor.}}{\Longrightarrow} \alpha^l \in \langle 1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\rangle \end{aligned}$$

und die Induktion ist vollständig.
b) $\sqrt{m}$ ist Nullstelle des quadratischen Polynoms $X^2 - m \in \mathbb{Q}[X]$, also algebraisch über $\mathbb{Q}$ und nach a) hat $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}[\sqrt{m}]$ höchstens den Grad 2 über $\mathbb{Q}$. Der Grad 1 kann nur für $m = 0$ oder $m = 1$ auftreten, denn für $m \ne 0$ 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.
Ist $\sqrt{m}$ oder $\sqrt{n}$ in $\mathbb{Q}$, so ist die Behauptung klar und der gesuchte Grad 1 oder 2.
Seien also im Folgenden $m, n \ne 0, \ne 1$ und daher $\sqrt{m}, \sqrt{n} \notin \mathbb{Q}$, also $k_m = \mathbb{Q}(\sqrt{m})$ und $k_n = \mathbb{Q}(\sqrt{n})$ quadratische Erweiterungen von $\mathbb{Q}$. Dann gilt $(k_m k_n : k_n) \le 2$ und daher $(k_m k_n : \mathbb{Q}) \le 2 \cdot (k_n : \mathbb{Q}) = 4$. Angenommen: $(k_m k_n : k_n) = 1$. Dann gilt

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

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

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

Also ist $(k_m k_n : k_n) = 2$ und $(k_m k_n : \mathbb{Q}) = 4$.
Daher ist das $\mathbb{Q}$-Erzeugendensystem $1, \sqrt{m}, \sqrt{n}, \sqrt{mn}$ von $k_m k_n = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ eine Basis.
Wir untersuchen nun $K = \mathbb{Q}(\sqrt{m} + \sqrt{n})$. Offenbar ist $K \subset k_m k_n$ und wegen $(\sqrt{m} + \sqrt{n})^2 = m + n + 2\sqrt{mn}$ ist $\mathbb{Q}(\sqrt{mn}) \subset K$. Also $K = k_m k_n$ 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 $K = k_m k_n$ hat den Grad 4.
c) Wir haben den Körperturm $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$, wobei jeder Schritt den Grad 2 hat: Der erste, weil $\sqrt{2}$ irrational ist, der dritte, weil i nicht reell ist, und der mittlere, weil $\sqrt[4]{2}$ nicht in $\mathbb{Q}(\sqrt{2})$ liegt:

$$\sqrt[4]{2} \in \mathbb{Q}(\sqrt{2}) \implies \bigvee_{r,s \in \mathbb{Q}} \sqrt{2} = (r + s\sqrt{2})^2 = r^2 + 2s^2 + 2rs\sqrt{2} \implies \sqrt{2} \in \mathbb{Q}\,,\ \text{Wid.}$$

Aufgabe 74.
Entfällt.

Algebra I
Übung 13

Aufgabe 75. (s)
Formulieren Sie möglichst viele Ansätze zur Einführung der komplexen Zahlen. Wiederholen Sie die hierbei auftretenden Begriffe.

Lösung:
1. Man definiert auf dem $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ die folgende Multiplikation: $(x_1, y_1) \cdot (x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$. Dann bildet $\mathbb{C} := (\mathbb{R}^2, +, \cdot)$ einen Körper mit Einselement $(1, 0)$ und imaginärer Einheit $i = (0, 1)$, $i^2 = -1$. Vermöge $r \mapsto (r, 0)$ wird $\mathbb{R}$ ein Teilkörper von $\mathbb{C}$.
2. Man definiert in der $\mathbb{R}$-Algebra $M_2(\mathbb{R})$ der 2-reihigen reellen Matrizen die Unteralgebra

$$\mathbb{C} := \{\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x, y \in \mathbb{R}\}.$$

Diese bildet einen Körper mit Einselement E und imaginärer Einheit $I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $I^2 = -E$. Es ist $\mathbb{C} = \mathbb{R} \cdot E \oplus \mathbb{R} \cdot I$ zweidimensionaler $\mathbb{R}$-Vektorraum und $\mathbb{R}$ vermöge $r \mapsto rE$ ein Teilkörper.
3. Man definiert im Polynomring $\mathbb{R}[X]$ das Hauptdideal $\mathfrak{a} := \langle X^2 + 1\rangle \lhd \mathbb{R}[X]$ und setzt

$$\mathbb{C} := \mathbb{R}[X]/\langle X^2 + 1\rangle$$

Dann ist $\mathbb{C}$ ein Körper ($X^2 + 1$ ist ein Primpolynom, $\mathfrak{a}$ in $\mathbb{R}[X]$ daher maximal). Vermöge $r \mapsto \bar{r} = r + \mathfrak{a}$ wird $\mathbb{R}$ ein Teilkörper und $i := \bar{X} \in \mathbb{C}$ eine Wurzel von $X^2 + 1$, also $i^2 = -1$.
Im Falle 1. müssen Assoziativität sowie Distributivität der Multiplikation nachgerechnet und die Existenz eines Inversen gezeigt werden. Im Falle 2. wird dies von der Matrixalgebra ererbt und die Invertierbarkeit ist mittels der Determinante sofort überprüfbar. Im Falle 3. sind natürlich einige Vorkenntnisse und Konstruktionen der Algebra Voraussetzung.

Aufgabe 76. (m)
Sei $\tilde{\mathbb{Q}}$ der algebraische Abschluss von $\mathbb{Q}$. Zeigen Sie:

a) $(\tilde{\mathbb{Q}} : \mathbb{Q}) = \infty$.

b) $\tilde{\mathbb{Q}}$ ist abzählbar.

c) Es existieren transzendente reelle Zahlen.

Lösung:
a) Die Polynome $X^n - 2 \in \mathbb{Q}[X]$ sind für alle n irreduzibel (Eisensteinkriterium) und daher $(\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}) = n$. $\tilde{\mathbb{Q}}$ enthält also Teilkörper beliebig hohen Grades, kann also selbst keinen endlichen Grad haben.
b) Alle Elemente von $\tilde{\mathbb{Q}}$ sind Wurzeln normierter rationaler Polynome, also ist

$$\tilde{\mathbb{Q}} = \bigcup_{n \in \mathbb{N}_+} \bigcup_{(a_0,\ldots,a_{n-1}) \in \mathbb{Q}^n} \{\alpha \in \tilde{\mathbb{Q}} \mid \sum_i a_i \alpha^i + \alpha^n = 0\}$$

abzählbare Vereinigung endlicher Mengen, also selbst abzählbar.
c) $\mathbb{R}$ ist überabzählbar, also $\mathbb{R} \setminus \tilde{\mathbb{Q}} \neq \emptyset$, es gibt nicht-algebraische Elemente über $\mathbb{Q}$.

Aufgabe 77. (s)
a) Seien $m, n \in \mathbb{Z}\setminus\{0,1\}$ quadratfrei (siehe Aufgabe 73 b)). Bestimmen Sie das Minimalpolynom von $\sqrt{m}+\sqrt{n}$ über $\mathbb{Q}$. Verwenden Sie dies zur Bestimmung des Minimalpolynoms von $(\sqrt{2}+\sqrt{3})i$ über $\mathbb{Q}$.
b) Zeigen Sie, dass für $x \in \mathbb{Q}$ $\cos(\pi x)$ und $\sin(\pi x)$ algebraisch sind über $\mathbb{Q}$. [Tipp: Komplexe Exponentialfunktion.]

Lösung:
a)Nach Aufgabe 73 b) ist $\mathbb{Q}(\sqrt{m}+\sqrt{n})$ vom Grade 4 über $\mathbb{Q}$. Es genügt also ein Polynom 4-ten Grades über $\mathbb{Q}$ zu finden, das $\alpha = \sqrt{m}+\sqrt{n}$ als Wurzel hat.

$$\begin{aligned} &\alpha^2 = (\sqrt{m}+\sqrt{n})^2 = m+n+2\sqrt{mn} \\ &\implies (\alpha^2 - m - n)^2 = 4mn \iff \alpha^4 - 2(m+n)\alpha^2 + (m+n)^2 - 4mn = 0 \end{aligned}$$

Damit ist $f_{\alpha,\mathbb{Q}} = X^4 - 2(m+n)X^2 + (m-n)^2$ das Minimalpolynom von α über $\mathbb{Q}$.
$(\sqrt{2}+\sqrt{3})i = \sqrt{-2}+\sqrt{-3}$ hat folglich das Minimalpolynom $X^4 + 10X^2 + 1$.
b) Sei $x = \frac{m}{n}$ mit $m, n \in \mathbb{Z}$, $n > 0$. Es gilt für $y \in \mathbb{R}$ $e^{iy} = \cos y + i \sin y$ und damit

$$(e^{i\pi x})^{2n} = (e^{i\pi \frac{m}{n}})^{2n} = e^{2\pi m \cdot i} = 1\,.$$

Daher ist $e^{\pm i\pi x}$ algebraisch über $\mathbb{Q}$ (eine $2n$-te Einheitswurzel). Dann sind auch

$$\cos(\pi x) = \frac{1}{2}(e^{i\pi x} + e^{-i\pi x}) \quad \text{und} \quad \sin(\pi x) = \frac{1}{2i}(e^{i\pi x} - e^{-i\pi x}) \quad \text{algebraisch.}$$

Aufgabe 78. (s)
Es sei $f = X^3 - 3X + 8 \in \mathbb{Q}[X]$.

a) Zeigen Sie, dass f irreduzibel über $\mathbb{Q}$, jedoch reduzibel über $\mathbb{R}$ ist.

b) Sei $K = \mathbb{Q}(\alpha)$ der Stammkörper von f über $\mathbb{Q}$. Stellen Sie α^{-1} und $\frac{1+\alpha}{1-\alpha}$ als Linearkombination der $\mathbb{Q}$-Basis $1, \alpha, \alpha^2$ dar.

Lösung:
a) Wäre das kubische Polynom f reduzibel über $\mathbb{Q}$, so müsste es eine rationale Nullstelle haben. Da f normiert ist, müsste diese Nullstelle ganzzahlig und ein Teiler von 8 sein. Keiner davon ist Nullstelle von f (siehe auch nachfolgende Überlegung).
Untersuchung über $\mathbb{R}$: Eine einfache schulbekannte Kurvendiskussion der reellen Funktion $x \mapsto f(x)$ zeigt: $f'(x) = 3(x^2-1)$ hat zwei einfache Nullstellen ± 1, die also Extremstellen von f sind. Wegen $\lim_{x\to\pm\infty} f(x) = \pm\infty$ ist $(+1, 6)$ ist lokaler Tiefpunkt und $(-1, 10)$ lokaler Hochpunkt. Die reelle Funktion $x \mapsto f(x)$ hat nach dem Zwischenwertsatz also genau eine Nullstelle im Bereich $x < -1$. f ist über $\mathbb{R}$ reduzibel.
b) Man 'beseitige' die Nenner, reduziere die auftretenden Potenzen von α mittels $\alpha^3 = 3\alpha - 8$ und löse dann das enstehende lineare Gleichungssystem über $\mathbb{Q}$:

$$\begin{aligned} \frac{1}{\alpha} = a + b\alpha + c\alpha^2 \quad &\iff 0 = c(3\alpha - 8) + b\alpha^2 + a\alpha - 1 = b\alpha^2 + (a+3c)\alpha - (1+8c) \\ &\iff b = 0\,,\ c = -\tfrac{1}{8}\,,\ a = \tfrac{3}{8} \\ \frac{1+\alpha}{1-\alpha} = a + b\alpha + c\alpha^2 \quad &\iff 0 = a + b\alpha + c\alpha^2 - a\alpha - b\alpha^2 - c(3\alpha - 8) - 1 - \alpha \\ &\iff 0 = (c-b)\alpha^2 + (b - a - 3c - 1)\alpha + a + 8c - 1 \\ &\iff b = c\,,\ a = 1 - 8c = -2c - 1 \iff b = c\,,\ c = \tfrac{1}{3}\,,\ a = -\tfrac{5}{3} \end{aligned}$$

Ergebnis:

$$\frac{1}{\alpha} = -\frac{1}{8}\alpha^2 + \frac{3}{8}\,, \quad \frac{1+\alpha}{1-\alpha} = \frac{1}{3}\alpha^2 + \frac{1}{3}\alpha - \frac{5}{3}\,.$$

Aufgabe 79. (s)
Es sei $\varphi : k \xrightarrow{\sim} k_1$ ein Isomorphismus von Körpern und $p(X) = \sum_{i=0}^{n} a_i X^i \in k[X]$ 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 $\varphi_1(\alpha) = \alpha_1$.

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. 63) die Isomorphismen

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

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.

Aufgabe 80. (s)
a) Zeigen Sie, dass $k := \mathbb{Z}[i]/7\mathbb{Z}[i]$ ein endlicher Körper ist. Tipp: Beachten Sie Aufgabe 61 .
b) Sei k_0 der Primkörper von k. Bestimmen Sie ein $\alpha \in k$ mit $k = k_0(\alpha)$ und sein Minimalpolynom.

Lösung:
a/b) Sei $R = \mathbb{Z}[i]$. Wir verwenden Aufgabe 61. 7 ist in R unzerlegbar, denn $7 = a^2 + b^2$ hat in $\mathbb{Z}$ keine Lösung und damit hat $\mathcal{N}(7) = 49$ keine Norm als echten Teiler. Da R faktoriell ist, ist 7 prim in R und das Ideal $7R$ maximal: $R/7R$ ist ein Körper. Sei $\varphi : R \twoheadrightarrow k = R/7R$ der natürliche Epimorphismus. Es ist $7R \cap \mathbb{Z} = 7\mathbb{Z}$ und damit $\varphi|_{\mathbb{Z}} : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/7\mathbb{Z} = \mathbb{F}_7$ der natürliche Epimorphismus. Es ist daher $k_0 = \mathbb{F}_7$ der Primkörper von k und $k = \varphi(\mathbb{Z}[i]) = \varphi(\mathbb{Z})[\varphi(i)] =: k_0[\alpha]$. Wegen $i^2 = 1$ folgt $\alpha^2 = 1$ und damit ist $k|k_0$ algebraisch höchstens vom Grad 2. Also ist k endlich.
Nun ist $X^2 + 1 \in \mathbb{F}_7[X]$ irreduzibel, da es keine Wurzel in $\mathbb{F}_7$ hat: Die Quadrate in $\mathbb{F}_7^\times$ sind $1, 2, 4$. Also ist $X^2 + 1$ das gesuchte Minimalpolynom und $(k : k_0) = 2$, $\#k = 49$.

Algebra I

Übung 14

Aufgabe 81. (m)
a) Sei K ein Körper und f ein Polynom über K vom Grad ≥ 1. Zeigen Sie: Ist $\mathrm{ggT}(f, f') = 1$, so gibt es kein Polynom g vom Grad ≥ 1 mit $g^2 \mid f$.
b) Zeigen Sie, dass $f = X^3 - 3X + 1$ in keinem Körper mehrfache Nullstellen hat.

Lösung:
a) Sei g ein Polynom mit $g^2 \mid f$, also $f = g^2 \cdot h$ mit $h \in K[X]$. Dann folgt $f' = 2gg'h + g^2h' = g(2g'h + gh')$, also ist g gemeinsamer Teiler von f und f'. Nach Voraussetzung muss g konstant sein.
b) $f' = 3X^2 - 3 = 3(X-1)(X+1)$ ist teilerfremd zu f, da ± 1 keine Wurzeln von f sind. Nach a) kann f also in keinem Körper einen Faktor $(X-a)^2$ haben.

Aufgabe 82. (m)
Seien p, q verschiedene Primzahlen und $k_p = \mathbb{Q}(\sqrt{p}) \subset \mathbb{R}$, analog k_q.
a) Zeigen Sie: $(k_p : \mathbb{Q}) = 2$.
b) $k_p \simeq k_q \iff p = q$.
Es gibt also unendlich untereinander nicht isomorphe Teilkörper von $\mathbb{R}$ vom Grade 2 über $\mathbb{Q}$.

Lösung:
Nach Aufgabe 73 b) gilt a) und $\sqrt{p} \in k_q \iff p = q$. Sei nun $\varphi : k_p \xrightarrow{\sim} k_q$. Wegen $\varphi(1) = 1$ ist $\varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$, so dass $\varphi(\sqrt{p})$ eine Wurzel von $X^2 - p$ in k_q sein muss, also $\varphi(\sqrt{p}) = \pm\sqrt{p} \in k_q$ und damit $p = q$.

Aufgabe 83. (s)
Sei $K|k$ eine Körpererweiterung vom Grade n und $\alpha \in K$. Zeigen Sie:

a) Die Linksmultiplikation $L_a : K \to K, x \mapsto a \cdot x$ ist ein Homomorphismus des k-Vektorraums K. Sei $A \in M_n(k)$ seine Matrix bzglèiner k-Basis $a_1, \ldots, a_n$ von K.

b) $f := \det(XE - A)$ ist ein normiertes Polynom vom Grade n über k mit $f(a) = 0$.

c) Ist f irreduzibel, so ist $K = k(a)$.

d) Bestimmen Sie das Minimalpolynom von $\sqrt[3]{2} + (\sqrt[3]{2})^2$ über $\mathbb{Q}$.

Lösung:
a) ist klar.
b) Es gilt $a \cdot a_i = \sum_{j=1}^n \alpha_{ij} a_j$ mit $a, a_i \in K$ und $\alpha_{ij} \in k$. Daraus folgt

$$0 = a \cdot a_i - \sum_{j=1}^n \alpha_{ij} a_j = \sum_{j=1}^n (a\delta_{ij} - \alpha_{ij}) a_j \text{ für } i = 1, \ldots, n\,.$$

Dies besagt, dass $(a_1, \ldots, a_n) \in K^n$ eine nicht-triviale Lösung des homogenen linearen Gleichungssystems mit der Matrix

$$(a\delta_{ij} - \alpha_{ij})_{ij} = aE - A \in M_n(K)$$

ist. Also muss $\det(aE - A) = 0$ sein, d. h. a ist Wurzel von $f(X) := \det(XE - A)$.

Nach Determinantendefinition ist

$$\begin{aligned}\det(XE-A) &= \underbrace{\prod_{i=1}^{n}(X-\alpha_{ii})}_{X^n-X^{n-1}\sum\alpha_{ii}+\ldots} + \sum_{\mathrm{id}\neq\sigma\in S_n}\prod_{\sigma i\neq i}\alpha_{i,\sigma i}\cdot\underbrace{\prod_{\sigma i=i}(X-\alpha_{ii})}_{\deg\leq n-2}\\ &= X^n - X^{n-1}\sum_i \alpha_{ii} + (\text{niedere Terme}) \in k[X]\end{aligned}$$

ein normiertes Polynom vom Grad n.
c) Ist f irreduzibel, so ist f das Minimalpolynom und $(k(a):k) = \deg f = n = (K:k)$, also $K = k(a)$.
d) Es ist $b = \sqrt[3]{2} + (\sqrt[3]{2})^2 \in K := \mathbb{Q}(\sqrt[3]{2})$ und wegen der Irreduzibilität von X^3-2 über $\mathbb{Q}$ ist eine $\mathbb{Q}$-Basis von K gegeben durch $a^i = (\sqrt[3]{2})^i$ $(i=0,1,2)$. Wegen $a^3 = 2$ hat L_a die Matrix $A_a = \begin{pmatrix}0&1&0\\0&0&1\\2&0&0\end{pmatrix}$ bzgl. der Basis a^i $(i=0,1,2)$. Dies ergibt für $L_b = L_a + L_{a^2} = L_a + L_a^2$ die Matrix

$$A_b = A_a + A_a^2 = \begin{pmatrix}0&1&0\\0&0&1\\2&0&0\end{pmatrix} + \begin{pmatrix}0&0&1\\2&0&0\\0&2&0\end{pmatrix} = \begin{pmatrix}0&1&1\\2&0&1\\2&2&0\end{pmatrix}$$

und damit nach b) das charakteristische Polynom

$$f(X) = \det\begin{pmatrix}X&-1&-1\\-2&X&-1\\-2&-2&X\end{pmatrix} = X^3 - 6X - 6\,.$$

Dieses ist irreduzibel über $\mathbb{Q}$, da f keine rationale Nullstelle hat (kein Teiler von 6 ist Nullstelle, siehe Aufgabe 67 b), also ist f das gesuchte Minimalpolynom.

Aufgabe 84. (s)

a) Sei G eine Gruppe und $a, b \in G$ vertauschbar, also $ab = ba$. Zeigen Sie: Haben a, b teilerfremde endliche Ordnungen m bzw. n, so hat ab die Ordnung mn.

b) Ist G endlich und abelsch mit $\#G = \exp G$, so ist G zyklisch.

c) Folgern Sie: Endliche Untergruppen in Multiplikationsgruppen $K^\times$ von Körpern sind zyklisch. [Tipp: Betrachten Sie für $e = \exp G$ das Polynom $X^e - 1$.]

Lösung:
a) Wegen der Vertauschbarkeit von a und b gilt $(ab)^{mn} = a^{mn}b^{mn} = e$, also $\mathrm{ord}(ab) \mid mn$. Sei nun $k = \mathrm{ord}(ab)$. Dann folgt

$$e = (ab)^{km} = a^{km}b^{km} = b^{km} \implies \mathrm{ord}\, b = n \mid km \underset{\mathrm{ggT}(m,n)=1}{\Longrightarrow} n = \mathrm{ord}\, b \mid k\,.$$

Genauso schließt man $m = \mathrm{ord}\, a \mid k$ und wegen der Teilerfremdheit von m und n folgt $mn \mid k = \mathrm{ord}(ab)$, womit a) bewiesen ist.
b) Sei $a \in G$ mit $\mathrm{ord}\, a = p_1^{\nu_1}\cdot\ldots\cdot p_r^{\nu_r}$ maximal. Annahme: $\mathrm{ord}\, a < \#G$, also nach Voraussetzung $\mathrm{ord}\, a < \#G = \exp G = \mathrm{kgV}\{\mathrm{ord}\, b \mid b \in G\}$. Dann gibt es ein $b \in G$ mit $\mathrm{ord}\, b \nmid \mathrm{ord}\, a$. Also $\mathrm{ord}\, a = p_1^{\nu_1}\cdot\ldots\cdot p_r^{\nu_r}$, $\mathrm{ord}\, b = p_1^{\mu_1}\cdot\ldots\cdot p_r^{\mu_r}$ mit verschiedenen Primzahlen p_i und o. E. $\mu_1 > \nu_1$. Dann folgt

$$\begin{aligned} a' = a^{p_1^{\nu_1}} &\quad \text{hat die Ordnung} \quad p_2^{\nu_2}\cdot\ldots\cdot p_r^{\nu_r}\,,\\ b' = b^{p_2^{\mu_2}\cdots p_r^{\mu_r}} &\quad \text{hat die Ordnung} \quad p_1^{\mu_1}\,.\end{aligned}$$

Damit haben a', b' teilerfremde Ordnungen und nach a) folgt

$$\operatorname{ord}(a'b') = p_1^{\mu_1} \cdot p_2^{\nu_2} \cdots p_r^{\nu_r} > \operatorname{ord} a$$

im Widerspruch zur Maximalität von $\operatorname{ord} a$.
c) Sei $G \leq K^\times$ endliche Untergruppe und $e := \exp G$ deren Exponent. Nach dem Satz von Lagrange wissen wir $e \leq \#G$. Nach Definition des Exponents gilt für alle $x \in G$ $x^e = 1$. Ganz G besteht also aus Nullstellen des Polynoms $X^e - 1 \in K[X]$ und daher gilt $\#G \leq e = \exp G \leq \#G$, $\exp G = \#G$. Nach b) folgt die Behauptung.

Aufgabe 85.
Siehe Prop. III.2.2.

Algebra I
Übung 15

Aufgabe 86.
Alle Körper dieser Aufgabe seien Teilkörper eines algebraisch abgeschlossenen Körpers Ω. Zeigen Sie:

a) Ist N über k endlich und normal, so auch über jedem Zwischenkörper L von $N|k$.

b) Ist $N|k$ endlich und normal, so ist für jede Erweiterung $L|k$ auch $NL|L$ endlich und normal.

c) Sind $N_1|k$ und $N_2|k$ endlich und normal, so gilt dies auch für $N_1N_2|k$ und $N_1 \cap N_2|k$.

d) Zu jeder endlichen Erweiterung $K|k$ gibt es eine endliche normale Erweiterung $N|k$ mit $K \subset N$.

Lösung:
Wir verwenden die Charakterisierungen aus Prop. III.2.7.
a) $N|k$ ist normal, also Zerfällungskörper eines Polynoms $f \in k[X]$. Da f auch in $L[X]$ liegt, ist $N|L$ normal.
b) $N|k$ normal, also wird N erzeugt von der Wurzelmenge $W_f := W_{f,\tilde{k}}$ eines Polynoms $f \in k[X] \subset L[X]$. Dann ist $KL = L[W_f]$ normal über L.
c) Es gilt $N_i = k[W_{f_i}]$ mit $f_i \in k[X]$ $(i = 1, 2)$, also $N_1N_2 = k[W_{f_1} \cup W_{f_2}] = k[W_f]$ mit $f = f_1f_2 \in k[X]$.
Sei $a \in N_1 \cap N_2$. Dann zerfällt das Minimalpolynom $f_{a,k}$ über N_1 und über N_2 in Linearfaktoren, also liegen alle Wurzeln bereits in $N_1 \cap N_2$.

Aufgabe 87.
Welche der folgenden Körper sind galoissch über $\mathbb{Q}$?

$$K_1 = \mathbb{Q}(\sqrt{2})\,, \quad K_2 = \mathbb{Q}(\sqrt[4]{2})\,, \quad K_3 = \mathbb{Q}(\sqrt[4]{2}, i)\,, \quad K_4 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$
$$\text{und} \quad K_5 = \mathbb{Q}(\alpha) \text{ mit } \alpha \in \mathbb{R} \text{ Wurzel von } f = X^3 - 3X + 8\,.$$

Lösung:
Da über Körpern der Charakteristik 0 alle Erweiterungen separabel sind, ist nur die Normalität zu untersuchen.
K_1 ist Zerfällungskörper von $X^2 - 2$, also galoissch.
$f = X^4 - 2$ ist irreduzibel (Eisensteinpolynom für $p = 2$), also das Minimalpolynom von $\sqrt[4]{2} \in K_2$. Aber f hat eine imaginäre Wurzel $i\sqrt[4]{2} \notin K_2$, also ist K_2 nicht normal.
$f = X^4 - 2$ hat in K_3 die 4 Wurzeln $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$. Diese erzeugen $K_3|^Q bb$, also ist K_3 der Zerfällungskörper von f und somit normal.
K_4 ist der Zerfällungskörper von $(X^2 - 2)(X^2 - 3)$.
K_5 ist nicht normal über $\mathbb{Q}$, denn f ist irreduzibel über $\mathbb{Q}$, hat α als einzige reelle Wurzel (vgl. Aufgabe 78), so dass die beiden anderen (komplexen) Wurzeln von f nicht in K_5 liegen, K_5 ist daher nicht normal.

Aufgabe 88.
Gegeben sind die über $\mathbb{Q}$ galoisschen Erweiterungen $N_1 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ und $N_2 = \mathbb{Q}(\sqrt[4]{2}, i)$ (siehe vorangehende Aufgabe).

a) Zeigen Sie $G_1 := G(N_1|\mathbb{Q}) \simeq \mathcal{V}_4$ und bestimmen Sie alle Untergruppen der Galoisgruppe, alle Zwischenkörper der Körpererweiterung sowie die Zuordnung zueinander gemäß dem Hauptsatz der Galoistheorie.

b) Zeigen Sie $G_2 := G(N_2|\mathbb{Q}) \simeq D_8$ und geben Sie Diagramme für den Untergruppenverband sowie den anti-isomorphen Zwischenkörperverband an.

Lösung:
a) Es ist $\#G_1 = (N_1 : \mathbb{Q}) = 4$ und die 4 Automorphismen von N_1 sind eindeutig festgelegt durch die 4 möglichen Bilder $(\pm\sqrt{2}, \pm\sqrt{3})$ von $\sqrt{2}, \sqrt{3}$:

$$\begin{aligned}
\sigma_{++} = \mathrm{id}: &\quad \sqrt{2} \mapsto +\sqrt{2}\,,\ \sqrt{3} \mapsto +\sqrt{3}\,,\\
\sigma_{+-}: &\quad \sqrt{2} \mapsto +\sqrt{2}\,,\ \sqrt{3} \mapsto -\sqrt{3}\,,\\
\sigma_{-+}: &\quad \sqrt{2} \mapsto -\sqrt{2}\,,\ \sqrt{3} \mapsto +\sqrt{3}\,,\\
\sigma_{--}: &\quad \sqrt{2} \mapsto -\sqrt{2}\,,\ \sqrt{3} \mapsto -\sqrt{3}\,,
\end{aligned}$$

Für jedes mögliche σ gilt also $\sigma^2 = \mathrm{id}$, so dass G_1 die Kleinsche Vierergruppe $\mathcal{V}_4$ sein muss (und nicht zyklisch ist). Die Untergruppen von $G_1 \simeq \mathcal{V}_4$ sind neben G_1 und $\{\mathrm{id}\}$ die drei Untergruppen der Ordnung 2 erzeugt von den drei Automorphismen $\neq \mathrm{id}$. Die zugehörigen Fixkörper sind $\mathbb{Q} = \mathrm{Fix}(G_1)$, $N_1 = \mathrm{Fix}(\mathrm{id})$ und wegen $\sigma_{+-}(\sqrt{2}) = \sqrt{2}$ bzw. $\sigma_{-+}(\sqrt{3}) = \sqrt{3}$ gilt $\mathbb{Q}(\sqrt{2}) = \mathrm{Fix}(\sigma_{+-})$, $\mathbb{Q}(\sqrt{3}) = \mathrm{Fix}(\sigma_{-+})$. Wegen $\sqrt{2}\sqrt{3} = \sqrt{6}$ enthält N_1 noch einen dritten quadratischen Teilkörper $\mathbb{Q}(\sqrt{6})$, der wegen $\sigma_{--}(\sqrt{6}) = \sqrt{6}$ der Fixkörper von σ_{--} sein muss. Damit sind nach dem Hauptsatz der Galoistheorie alle Zwischenkörper erfasst.
b) $\mathbb{Q}(\sqrt[4]{2}, i)$ ist galoissch über $\mathbb{Q}$ vom Grad 8, denn $K := \mathbb{Q}(\sqrt[4]{2})$ hat über $\mathbb{Q}$ den Grad 4 ($X^4 - 2$ irreduzibel) und $N_1 = K(i)$ über K den Grad 2 ($i \notin K \subset \mathbb{R}$). Also ist G_2 eine Gruppe der Ordnung 8. Die Diedergruppe D_8 ist die nicht-abelsche Gruppe der Ordnung 8 erzeugt von einem Element σ der Ordnung 4 und einem Element $\tau \neq \sigma^2$ der Ordnung 2 (siehe Gruppen spezieller Ordnung A)).
$N_2|\mathbb{Q}(i)$ ist galoissch vom Grade 4 und $G(N_2|\mathbb{Q}(i)) = \langle\sigma\rangle$ mit σ definiert durch $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$. $N_2 = K(i)$ ist galoissch über K vom Grade 2 und $G(N_2|K) = \langle\tau\rangle$ mit $\tau(i) = -i$. Diese beiden Automorphismen $\sigma, \tau \in G_2$ erzeugen G_2, denn

$$\mathrm{Fix}\langle\sigma,\tau\rangle \subset \mathrm{Fix}(\sigma,\tau) = \mathrm{Fix}(\sigma) \cap \mathrm{Fix}(\tau) = \mathbb{Q}(i) \cap \mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q} = \mathrm{Fix}(G_2)\,,$$

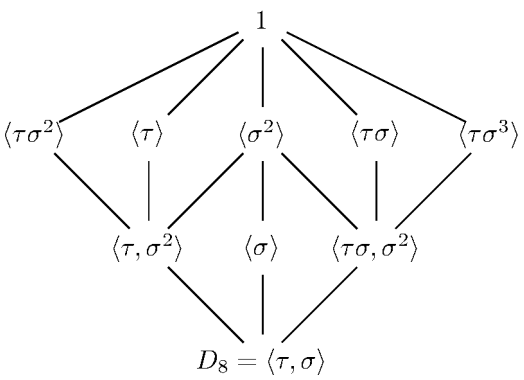
also $\mathrm{Fix}\langle\sigma,\tau\rangle = \mathrm{Fix}(G_2)$ und nach dem Hauptsatz folgt $G_2 = \langle\sigma,\tau\rangle$. Die Gruppe G_2 ist nicht abelsch, denn

$$\tau\circ\sigma : \sqrt[4]{2} \mapsto -i\sqrt[4]{2}\,, \quad \sigma\circ\tau : \sqrt[4]{2} \mapsto i\sqrt[4]{2}\,,$$

Wegen $\tau(i) = -i$ gilt $\tau \notin \langle\sigma\rangle$. Damit ist G_2 die Diedergruppe D_8.
Die Untergruppen von D_8: Wir kennen neben der trivialen und der vollen Gruppe die 5 Untergruppen der Ordnung 2 erzeugt von $\sigma^2 \in \mathrm{Zentr}(D_8)$ bzw. $\tau\sigma^\nu$ ($\nu = 0, \ldots, 3$) und die Untergruppe von der Ordnung 4, Normalteiler, erzeugt von σ (siehe wieder Vorlesung loc.cit). Wegen $\sigma^2 \in \mathrm{Zentr}(D_8)$ sind auch $\langle\tau, \sigma^2\rangle$ und $\langle\tau\sigma, \sigma^2\rangle$ Untergruppen der Ordnung 4 (Kleinsche Vierergruppen). Nachfolgend ist nun das Diagramm des Untergruppenverbandes von D_8 „kopfüber“

dargestellt, also mit der trivialen Gruppe oben und der vollen Gruppe unten.

Untergruppenverband D_8
(„kopfüber“)



Nach dem Hauptsatz der Galoistheorie stellt dieses Diagramm auch den Zwischenkörperverband der Galoiserweiterung $\mathbb{Q}(i,\sqrt[4]{2})$ (in üblicher Darstellung, unten $\mathbb{Q}$, oben $\mathbb{Q}(i,\sqrt[4]{2})$) dar. Wir wollen nun der Vollständigkeit halber die Zuordnung von Untergruppe zu Fixkörper aufklären. Einige der zugehörigen Fixkörper sind per definitionem klar:

$$\mathrm{Fix}(\sigma)=\mathbb{Q}(i)\,,\quad \mathrm{Fix}(\tau)=\mathbb{Q}(\sqrt[4]{2})\,.$$

Wegen $\sigma^2(\sqrt[4]{2})=-\sqrt[4]{2}$ ist $\sigma^2(\sqrt{2})=\sqrt{2}$, so dass durch Gradvergleich folgt

$$\mathrm{Fix}(\sigma^2)=\mathbb{Q}(i,\sqrt{2})\,,$$

Zur Bestimmung der Fixkörper der drei übrigen Involutionen $\tau\sigma^\nu$ $(\nu=1,2,3)$ berechnen wir

$$\tau\sigma:\begin{cases}\sqrt[4]{2}\mapsto -i\sqrt[4]{2}\\ i\sqrt[4]{2}\mapsto -\sqrt[4]{2}\end{cases}\qquad \tau\sigma^2:\begin{cases}\sqrt[4]{2}\mapsto -\sqrt[4]{2}\\ i\sqrt[4]{2}\mapsto i\sqrt[4]{2}\end{cases}\qquad \tau\sigma^3:\begin{cases}\sqrt[4]{2}\mapsto i\sqrt[4]{2}\\ i\sqrt[4]{2}\mapsto \sqrt[4]{2}\end{cases}$$

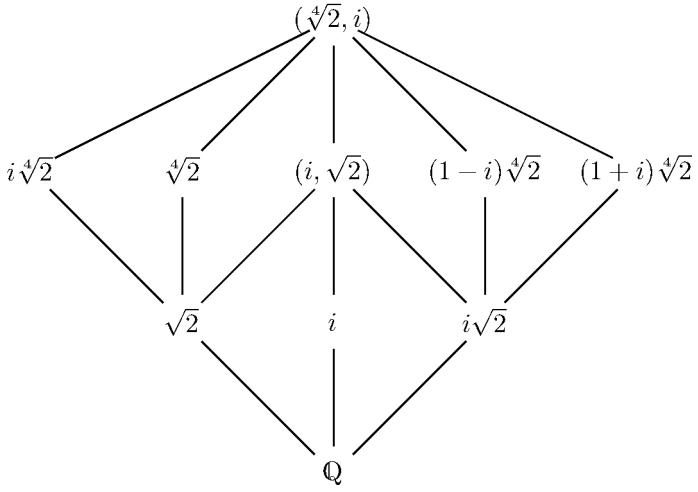
so dass wir die folgenden Fixelemente und damit die jeweiligen Fixkörper vom Grade 4 (!) erkennen können:

$$\mathrm{Fix}(\tau\sigma^2)=\mathbb{Q}(i\sqrt[4]{2})\,,\quad \mathrm{Fix}(\tau\sigma)=\mathbb{Q}(\sqrt[4]{2}(1-i))\,,\quad \mathrm{Fix}(\tau\sigma^3)=\mathbb{Q}(\sqrt[4]{2}(1+i))\,.$$

Wegen $((1\pm i)\sqrt[4]{2})^4=-8$ sind die letzten beiden Körper isomorph zum Stammkörper $\mathbb{Q}(\sqrt[4]{-8})$ von X^4+8.

Nachfolgend nun der Zwischenkörperverband von $\mathbb{Q}(i,\sqrt[4]{2})|\mathbb{Q}$ in einem Diagramm, das die Zuordnungen zum obigen Untergruppendiagramm genau wiedergibt. Der Übersichtlichkeit halber sind in diesem Diagramm nur die erzeugenden Elemente über $\mathbb{Q}$ notiert.

Zwischenkörperverband $\mathbb{Q}(\sqrt[4]{2},i)$
(erzeugende Elemente)



Aufgabe 89.
Sei p eine Primzahl. Zeigen Sie:

a) Sei $f \in \mathbb{Q}[X]$ irreduzibel vom Grad p mit genau zwei nicht-reellen Nullstellen. Dann hat der Zerfällungskörper N von f die symmetrische Gruppe $\mathcal{S}_p$ als Galoisgruppe. [Tipp: Aufgabe 20 d).]

b) Für $m \in \mathbb{N}$, $m \geq 2$ sei $f = X^5 - mpX + p$ und N der Zerfällungskörper über $\mathbb{Q}$. Bestimmen Sie die Galoisgruppe $G(N|\mathbb{Q})$.

Lösung:
a) Als irreduzibles Polynom ist f separabel (Charakteristik 0) und der Zerfällungskörper wird von den p verschiedenen Wurzeln von f erzeugt. Die Galoisgruppe operiert auf den p Wurzeln und $G(N|\mathbb{Q})$ wird so in $\mathcal{S}_p$ eingebettet. Wir wollen zeigen, dass dies ein Isomorphismus ist. Gemäß dem Hinweis genügt es in $G(N|\mathbb{Q})$ einen p-Zyklus und eine Transposition zu finden. Da f genau zwei nicht-reelle Wurzeln hat, werden diese von der komplexen Konjugation vertauscht und die übrigen Wurzeln bleiben fest, also operiert die komplexe Konjugation als Transposition auf den Wurzeln von f.
Andererseits sind in $\mathcal{S}_p$ die p-Zyklen genau die Elemente der Ordnung p und $G(N|\mathbb{Q})$ muss ein solches Element enthalten, weil die Gruppenordnung durch p teilbar ist: Ist nämlich $K = \mathbb{Q}(\alpha) \subset N$ ein Stammkörper von f, so gilt $p = \deg f = (K : \mathbb{Q}) \mid (N : \mathbb{Q}) = \#G(N|\mathbb{Q})$.
Damit enthält $G(N|\mathbb{Q}) \hookrightarrow \mathcal{S}_p$ eine Transposition $(a_1\, a_2)$ und einen p-Zyklus. Durch die Potenzen eines p-Zykluses σ kann jedes Element auf jedes andere in $\{1, \ldots, p\}$ abgebildet werden, also auch $\sigma^j(a_1) = a_2$ für ein j. Mit σ ist auch jede Potenz $\sigma^j \neq \mathrm{id}$ ein p-Zyklus. Damit enthält G die Transposition $\tau = (a_1\, a_2)$ und einen p-Zyklus $\rho = (a_1, a_2, \ldots, a_p)$. Nach Aufgabe 20 d) muss G gleich $\mathcal{S}_p$ sein.
b) $f = X^5 - mpX + p$ ist irreduzibel (eisensteinsch für p), also $G(N|\mathbb{Q}) \subset \mathcal{S}_5$. Wir zeigen, dass f genau 3 reelle und folglich genau 2 nicht-reelle Nullstellen hat, so dass gemäß a) die Galoisgruppe $\mathcal{S}_5$ ist.
Die Ableitung $f'(x) = 5x^4 - mp$ der reellen Polynomfunktion f hat genau zwei reelle einfache Nullstellen $\pm\alpha$ mit $\alpha = \sqrt[4]{\frac{mp}{5}}$. $+\alpha$ ist Minimal- und $-\alpha$ Maximalstelle von f. Wir zeigen $f(-\alpha) > 0$ und $f(\alpha) < 0$, so dass f genau eine Nullstelle im Intervall $]-\alpha, \alpha[$ hat und wegen $\lim_{x\to\pm\infty} f(x) = \pm\infty$ jeweils genau eine weitere davor bzw. dahinter.
Die erste Bedingung ist immer erfüllt:

$$f(-\alpha) = -\alpha \cdot \frac{mp}{5} + mp\alpha + p = \frac{4}{5}\alpha mp + p > 0\,.$$

Wir untersuchen die zweite:

$$f(\alpha) = -\tfrac{4}{5}\alpha mp + p < 0 \iff \tfrac{4}{5}\alpha mp > p \iff \alpha m > \tfrac{5}{4}$$
$$\iff \alpha^4 m^4 = \tfrac{mp}{5} m^4 > \tfrac{5^4}{4^4} \iff m^5 p > \tfrac{5^5}{4^4}$$

Wegen $\frac{5^5}{4^4} < 13$ ist dies für $m \geq 2$ erfüllt (aber auch für $m = 1$ und $p \geq 13$).

Aufgabe 90. (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).

Aufgabe 91.
Beweisen Sie den

- **Fundamentalsatz der Algebra:** $\mathbb{C}$ ist algebraisch abgeschlossen.

nach der Idee von E. Artin mittels Sylowsätzen und Galoisscher Theorie allein auf der Basis des

- Zwischenwertsatzes der reellen Analysis.

Zeigen Sie dazu:

a) Jede positive reelle Zahl besitzt eine positive reelle Quadratwurzel.

b) Jede komplexe Zahl $z \in \mathbb{C}$ besitzt in $\mathbb{C}$ eine Quadratwurzel.

c) $\mathbb{R}$ besitzt keine echte algebraische Erweiterung ungeraden Grades.

Sei im Folgenden $K|\mathbb{C}$ eine endlich algebraische Erweiterung von $\mathbb{C}$ und N die galoissche Hülle von K *über* $\mathbb{R}$. Folgern Sie:

d) $G(N|\mathbb{R})$ ist eine 2-Gruppe.

e) Ist $H = G(N|\mathbb{C}) \neq 1$, so existiert eine Untergruppe $H' < H$ vom Index 2 und $\mathbb{C}$ besitzt eine quadratische Erweiterung.

Lösung:
a) Sei $a \in \mathbb{R}_+$ und $f(x) = x^2 - a$. Dann ist $f(0) = -a < 0$ und $f(b) > 0$ für $b > \max(a, 1)$, so dass f nach dem Zwischenwertsatz eine reelle Nullstelle in $]0, b[$ besitzt, also eine positive reelle Quadratwurzel aus a existiert.
b) Es sei $z = a + bi \in \mathbb{C}$ und o. E. $z \notin \mathbb{R}$, da für (alle!) reellen Zahlen Quadratwurzeln in $\mathbb{C}$ existieren. Da die komplexe Multiplikation geometrisch eine Drehstreckung ist, muss die gesuchte Quadratwurzel die Richtung der Winkelhalbierenden zwischen den Vektoren $z \in \mathbb{C}$ und $1 \in \mathbb{C}$ haben. Deren Richtung ist die Richtung des Summenvektors $z + |z|$, denn in Parallelogrammen mit gleich langen Seiten ist die Diagonale auch Winkelhalbierende.
Wir berechnen also

$$(z + |z|)^2 = a^2 - b^2 + 2abi + 2\,|z|\,z + a^2 + b^2 = 2(a + |z|) \cdot z =: \alpha \cdot z$$

mit $\alpha \in \mathbb{R}$. Wegen $b \neq 0$ ist $|z| > -a$, also $\alpha > 0$. Damit ist gezeigt:

$$\frac{1}{\sqrt{\alpha}}(z + |z|) \in \mathbb{C} \text{ ist Quadratwurzel von } z \in \mathbb{C} \setminus \mathbb{R}\,.$$

c) Sei $K|\mathbb{R}$ endlich algebraisch von ungeradem Grade $n > 1$. Wegen Charakteristik 0 ist die Erweiterung separabel und besitzt ein primitives Element a, also gilt $K = \mathbb{R}[a]$ und das Minimalpolynom $f := f_{a,\mathbb{R}}$ hat den ungeraden Grad $n = (K : \mathbb{R}) > 1$. Als reelle Polynomfunktion ungeraden Grades hat f dann eine reelle Nullstelle und kann nicht irreduzibel sein, Wid.
d) Wäre $\#G$ keine 2-Potenz, so wäre eine 2-Sylowgruppe S *echte* Untergruppe von G und hätte daher ungeraden Index $n > 1$ in G. Der Fixkörper von S wäre damit eine endliche Erweiterung von $\mathbb{R}$ vom Grade n; Wid. zu c).
e) Ist $1 \neq H = G(N|\mathbb{C}) < G = G(N|\mathbb{R})$, so ist $\#H = 2^k$ mit $k \geq 1$ und nach den Sylowsätzen existiert in H dann eine Untergruppe H' mit $\#H' = 2^{k-1}$, also $(H : H') = 2$. Der Fixkörper K' von H' wäre daher eine quadratische Erweiterung von $\mathrm{Fix}(H) = \mathbb{C}$.
Beweisschluss: Da quadratische Körpererweiterungen durch Quadratwurzeln erzeugt werden (für Charakteristik $\neq 2$), $\mathbb{C}$ aber alle Quadratwurzeln enthält, ist $K' = \mathbb{C}$, Wid. Also muss $H = 1$ trivial und damit $\mathbb{C} = \mathrm{Fix}(H) = \mathrm{Fix}(1) = N$ sein. $\mathbb{C}$ besitzt also keine echte algebraische Erweiterung K.