Blatt 1

1. Sei G eine Gruppe der Ordnung n. Sei $1 \in S \subset G$ eine Teilmenge. Zeige, dass
$$S^n = \{s_1 \cdots s_n : s_1, \ldots, s_n \in S\}$$
eine Untergruppe von G ist.

   Lösung. Sei $s \in S$. Die Abbildung $m_s : S^k \to S^{k+1}$, $x \mapsto sx$ ist injektiv, also folgt $|S^k| \leq |S^{k+1}|$. Ferner gilt $|S^k| = |S^{k+1}| \Rightarrow |S^{k+1}| = |S^{k+2}|$. Also gibt es ein k_0 mit
$$|S| < |S^2| < \cdots < |S^{k_0}| = |S^{k_0+1}| = \ldots$$
   Da die ersten Kardinalitäten echt ansteigen, gilt $|S^j| \geq j$ fuer $j = 1, \ldots, k_0$ und daher $k_0 \leq n$. Damit ist $S^n = S^{n+1} = \ldots$. Da jedes Element endliche Ordnung hat, ist dies eine Untergruppe. □

2. Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

   Lösung. Sei $G = \langle \tau \rangle$ eine zyklische Gruppe und sei $\{1\} \neq H \subset G$ eine Untergruppe. Sei N die kleinste natuerliche Zahl mit $\gamma = \tau^N \in H$. Wir zeigen, dass H von γ erzeugt ist. Sei hierzu $h = \tau^n \in H$, dann ist $h\gamma^k = \tau^{n+kN} \in H$. Es gibt ein $k \in \mathbb{Z}$ mit $0 \leq n + kN < N$. Aus der Minimalitaet von N folgt $n + kN = 0$ und daher $h = \gamma^{-k}$. □

3. Sei N ein zyklischer Normalteiler der Gruppe G und sei $H \subset N$ eine Untergruppe. Ist H ein Normalteiler in G?

   Lösung. Ja. Wir setzen $H \neq \{1\}$ voraus. Dann ist H selbst zyklisch und besteht damit genau aus den Elementen der Form n^k mit $n \in N$ und $k = |N/H|$. Ist also $h = n^k \in H$ und $g \in G$, dann ist $ghg^{-1} = \left(gng^{-1}\right)^k$ und da gng^{-1} wieder in N liegt, folgt $ghg^{-1} \in H$ und daher ist H normal. □

4. Wir sagen: Eine Gruppe G hat *Exponent* $m \in \mathbb{N}$, falls $x^m = 1$ für jedes $x \in G$ gilt. Fuer welche Primzahlen p gilt: Jede endliche Gruppe G mit Exponent p ist abelsch?

   Anwort: genau fuer $p = 2$.

   Lösung. Ist $p = 2$, so gilt $1 = abab = aba^{-1}b^{-1}$.

   Sei nun $p > 2$ und sei $\mathcal{N}$ die Menge der oberen 3×3 Matrizen über dem Körper $\mathbb{F}_p$ mit Nullen auf der Diagonale und sei $\mathcal{H} = I + \mathcal{N} = \{I + N : N \in \mathcal{N}\}$, wobei I die 3×3 Einheitsmatrix ist. Wir behaupten, dass $\mathcal{H}$ eine Gruppe vom Exponenten p ist. Nach LinA ist sie eine Untergruppe von $\mathrm{GL}_3(\mathbb{F}_p)$. Ist $N = \begin{pmatrix} 0 & x & y \\ & 0 & z \\ & & 0 \end{pmatrix}$, dann ist
$$N^2 = \begin{pmatrix} 0 & 0 & xz \\ & 0 & 0 \\ & & 0 \end{pmatrix}, \quad N^3 = 0.$$

Damit also auch $N^p = 0$ (da $p > 2$!) und daher

$$(I+N)^p = \sum_{k=0}^{p} \binom{p}{k} N^k = I + pN + \frac{p(p-1)}{2} N^2 = I,$$

denn in $\mathbb{F}_p$ gilt $p = 0$. (An dieser Stelle geht wieder $p > 2$ ein!) Damit hat die Gruppe $\mathcal{H}$ den Exponenten p. Sie ist allerdings nicht abelsch, da

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

aber

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

Blatt 2

1. Die Gruppe G operiere auf der Menge X. Seien $g \in G$, $x \in X$. Zeige, dass
$$gG_xg^{-1} = G_{g.x}.$$

   Lösung. Fuer gegebenes $h \in G$ gilt
$$\begin{aligned} h \in G_x &\Leftrightarrow hgx = gx \\ &\Leftrightarrow g^{-1}hgx = x \\ &\Leftrightarrow g^{-1}hg \in G_x \\ &\Leftrightarrow h \in gG_xg^{-1}. \end{aligned}$$
   □

2. Seien $H \subsetneq G$ endliche Gruppen. Zeige
$$G \neq \bigcup_{g \in G} gHg^{-1}.$$

   Lösung. Sei $R = \bigcup_{g\in G} gHg^{-1}$ und sei $(g_1, \ldots, g_n)$ ein Vertretersystem von G/H, also $G = \bigsqcup_{j=1}^{n} g_jH$. Wegen $H \neq G$ ist $n \geq 2$. Die Abbildung
$$\begin{aligned} \phi : G/H \times H &\to R, \\ (g_jH, h) &\mapsto g_jhg_j^{-1} \end{aligned}$$
   ist surjektiv, aber nicht injektiv, da $\phi(g_jH, 1) = 1$ fuer jedes $j = 1, \ldots, n$. Daher folgt
$$|R| < |G/H \times H| = |G|.$$
   □

3. Eine Gruppenoperation heisst *transitiv*, falls es nur eine Bahn gibt.

   Eine endliche Gruppe G operiere transitiv auf einer Menge X, so dass jedes $g \in G$ mindestens einen Fixpunkt in X hat, d.h., zu jedem $g \in G$ gibt es ein $x \in X$ mit $gx = x$. Zeige, dass X aus nur einem Punkt besteht.

   Lösung. Sei $x \in X$ und H der Stabilisator von x. Dann ist X in G-aequivarianter Bijektion zu G/H. Ist nun $g \in G$, dann gibt es also ein $x \in G$ mit $gxH = xH$, also $g \in xHx^{-1}$. Da g beliebig war, folgt $G = \bigcup_{x\in G} xHx^{-1}$ und damit nach der letzten Aufgabe $H = G$. □

4. Sei G eine Gruppe und sei $\mathrm{Inn}(G)$ die Menge aller *inneren Automorphismen* von G, d.h., die Menge aller Abbildungen der Form
$$\begin{aligned} C_g : G &\to G, \\ x &\mapsto gxg^{-1} \end{aligned}$$
   mit $g \in G$. Zeige dass $\mathrm{Inn}(G)$ in $\mathrm{Aut}(G)$ liegt und ein Normalteiler in dieser Gruppe ist.

   Lösung. Als erstes zeigen wir, dass jedes C_g ein Automorphismus ist. Es gilt $G_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = C_g(x)C_g(y)$, also ist C_g ein

Gruppenhomomorphismus. Weiter ist $C_g C_{g^{-1}}(x) = gg^{-1}xgg^{-1} = x$, also ist $\mathrm{Inn}(G)$ eine Untergruppe von $\mathrm{Aut}(G)$. Ist $\phi \in \mathrm{Aut}(G)$, so gilt

$$\phi \circ C_g \circ \phi^{-1}(x) = \phi\Big(g\phi^{-1}(x)g^{-1}\Big) = \phi(g)\phi\Big(\phi^{-1}(x)\Big)\phi(g)^{-1} = \phi(g)x\phi(g)^{-1} = C_{\phi(g)}(x).$$

Das heisst also $\phi\,\mathrm{Inn}(G)\phi^{-1} \subset \mathrm{Inn}(G)$ und damit ist $\mathrm{Inn}(G)$ ein Normalteiler. □

Blatt 3

1. Sei G eine unendliche Gruppe. Ist H eine Untergruppe, dann nennen wir die Zahl $|G/H| \in \mathbb{N}_0 \cup \{\infty\}$ den *Index* von H in G. Zeige:

   (a) Haben die Untergruppen A, B endlichen Index, so auch ihr Schnitt $A \cap B$ und es gilt $|G/A \cap B| \leq |G/A|\,|G/B|$.

   (b) Hat die Untergruppe H endlichen Index, dann enthaelt H einen Normalteiler von endlichem Index.

   Lösung. (a) Die Gruppe A operiert transitiv auf der Menge AB/B und der Stabilisator von B ist $A \cap B$. Daher ist $|A/A \cap B| = |AB/B| \leq |G/B|$.

   Ist $G = \bigsqcup_{j=1}^{n} g_j A$, dann folgt $G/A \cap B = \sqcup_{j=1}^{n} g_j A/A \cap B$ und daher ist $|G/A \cap B| = n|A/A \cap B| = |G/A||A/A \cap B| = |G/A|\,|AB/B| \leq |G/A|\,|G/B|$

   (b) Sei $G = \bigcup_{j=1}^{n} g_j H$ und sei $N = \bigcap_{g \in G} gHg^{-1} = \bigcap_{j=1}^{n} g_j H g_j^{-1}$. Dieser Schnitt ist normal und hat nach (a) endlichen Index in G. □

2. Sei G eine endliche Gruppe und p der kleinste Primteiler der Gruppenordnung. Die Gruppe G habe einen Normalteiler N der Ordnung p. Zeige, dass G ein nichttriviales Zentrum hat.

   Lösung. Sei τ ein Erzeuger von N. Dann ist $g\tau g^{-1}$ fuer $g \in G$ ebenfalls ein Erzeuger von N. Das bedeutet, dass G die Menge der Erzeuger $\mathcal{E}$ permutiert. Es gilt $\mathcal{E} = N \setminus \{1\}$ und damit $|\mathcal{E}| = p - 1$. Jedes G-Orbit in $\mathcal{E}$ hat daher eine Mächtigkeit $m < p$. Andererseits muss m ein Teiler der Gruppenordnung sein. Da p aber der kleinste nichttriviale Teiler ist, folgt $m = 1$ also ist jedes Element von N zentral. □

3. Seien $m, n \in \mathbb{N}$. Gib eine vollstaendige Liste aller Gruppen der Ordnung ≤ 7 bis auf Isomorphie (mit Beweis!).
   (Hinweis: Ist G eine nichabelsche Gruppe der Ordnung 6, dann operiert G auf der Menge seiner 2-Sylow-Gruppen.)

   Lösung. Zur Ordnung 1 gibt es nur eine Gruppe, die triviale. Die Zahlen 2,3,5,7 sind Primzahlen, also gibt es jeweils nur die zyklische Gruppe.

   $n = 4$: Hat G ein Element der Ordnung 4, dann ist G zyklisch. Hat es keines, dann hat jedes nichttriviale Element die Ordnung 2. Damit ist G abelsch. Seien a, b zwei verschiedene nichttriviale Elemente. Dann ist ab ebenfalls nichttrivial und das waeren dann alle Elemente. Daher ist die Abbildung

   $$\begin{aligned} \phi : \mathbb{Z}/2 \times \mathbb{Z}/2 &\to G, \\ (k, l) &\mapsto a^k b^l \end{aligned}$$

   ein Gruppenisomorphismus.

   $n = 6$: Eine Gruppe G der Ordnung 6 operiert auf der Menge ihrer 2-Sylow-Gruppen. Sei s die Anzahl der 2-Sylow-Gruppen. Dann ist s ungerade und muss aus anzahltechnischen Gruenden ≤ 5 sein. Sie kann aber nicht 5 sein, da dann alle Elemente die Ordnung 2

haetten, es muss aber ein Element b der Ordnung 3 geben. Ist $s = 1$, dann ist die 2-Sylow-Gruppe $\langle a \rangle$ zentral, vertauscht also mit b, so dass die Abbildung $\mathbb{Z}/2 \times \mathbb{Z}/3 \to G$, $(k, l) \mapsto a^k b^l$ ein Isomorphismus ist. Ist $s = 3$, dann permutiert G diese drei und wir erhalten einen nichttrivialen Homomorpohismus $\phi : G \to \mathrm{Per}(3)$. Da G transitiv auf den 2-Sylows operiert, hat der Kern maximal 2 Elemente. Es gibt also zwei verschiedene Elemente der Ordnung 2 im Bild von ϕ. Solche zwei erzeugen aber ganz Per(3), also ist ϕ ein Isomorphismus. □

4. Sei K ein Koerper und sei $n \in \mathbb{N}$. Zeige, dass die Gruppe G der oberen Dreiecks-$n \times n$-Matrizen mit Einsen auf der Diagonale nilpotent ist.

   Lösung. Sei U_m die Menge aller Matrizen N mit

   $$N_{i,j} \neq 0 \quad \Rightarrow \quad i + m < j.$$

   Wir zeigen: mit $U = U_0$ gilt $U_0 U_m \subset U_{m+1}$ und $U_m U_0 \subset U_{m+1}$. Hierzu sei $M \in U_0$ und $N \in U_m$. Seien $1 \leq i, j \leq n$ mit $(MN)_{i,j} \neq 0$, also

   $$0 \neq (MN)_{i,j} = \sum_{k=1}^{n} M_{i,k} N_{k,j} = \sum_{k=i+1}^{j-m-1} M_{i,k} N_{k,j}$$

   Diese Summe ist nur dann nichttrivial, wenn $i + m + 1 < j$, womit $U_0 U_m \subset U_{m+1}$ folgt. Die andere Reihenfolge geht genauso.

   Fuer $m \in \mathbb{N}_0$ sei nun $G_m = \mathbf{1} + U_m \subset G$. Dann ist $G = G_0$ und $G_n = \{\mathbf{1}\}$. Wir zeigen, dass G_m eine Untergruppe ist: Fuer $A = \mathbf{1} - N \in G_m$ ist N eine nilpotente Matrix, also $N^n = 0$ und damit

   $$(1 - N) \sum_{k=0}^{n} N^k = 1.$$

   Also ist A^{-1} wieder in G_m.

   Wir behaupten $[G, G_m] \subset G_{m+1}$. Seien $A = \mathbf{1} + M \in G$ und $B = \mathbf{1} + N \in G_m$. Wir schreiben $M' = M + M^2 + \cdots + M^n$ und erhalten $MM' = M' - M$ und ebenso fuer N. Ferner gilt $(1-M)^{-1} = 1+M'$ und $(1-N)^{-1} = 1+N'$. Dann ist

   $$[A, B] = (\mathbf{1} - M)(\mathbf{1} - N)(\mathbf{1} + M)^{-1}(\mathbf{1} + N)^{-1} = (\mathbf{1} - M)(\mathbf{1} - N)(\mathbf{1} + M')(\mathbf{1} + N').$$

   Das kann man jetzt ausmultiplizieren. Beachte aber, dass jedes Produkt mit mindestens zwei Faktoren, das N oder N' enthaelt, schon in U_{m+1} liegt. Wir erhalten also ein $R \in U_{m+1}$ so dass

   $$\begin{aligned} [A, B] &= \mathbf{1} - M - N + M' + N' - MM' - NN' + R \\ &= \mathbf{1} - M - N + M' + N' - M' + M - N' + N + R = 1 + R. \end{aligned}$$ □

Blatt 4

1. Sei F_2 die freie Gruppe in zwei Erzeugern a, b.

   (a) Zeige, dass es für jedes Element $z \in F_2$ Zahlen $k, l \in \mathbb{Z}$ gibt, so dass
   $$z = a^l b^l \, k_1 \cdots k_r,$$
   wobei die k_j Kommutatoren sind.

   (b) Zeige:
   $$F_2^{\mathrm{ab}} \cong \mathbb{Z}^2.$$

   Lösung. (a) Jedes Element z von F_2 ist ein Produkt von Faktoren der Form a, b, a^{-1}, b^{-1}. Wir zeigen die Behauptung durch Induktion nach der Anzahl der Faktoren. Ist diese Zahl Null, dann ist $z = 1$ und die Behauptung gezeigt. Sei also $z = a^{\pm 1} w$ für ein Wort w, das die Behauptung erfüllt, dann erfüllt z sie auch. Ist $z = b^{\pm 1} w$ mit einem w, das die Behauptung erfüllt, also etwa $w = a^k b^l m$, wobei m ein Produkt von Kommutatoren ist, dann gilt

   $$z = b^{\pm 1} a^k b^l m = a^k b^{\pm 1} \, [b^{\mp 1}, a^k] \, b^l \, m = a^k b^{l \pm 1} \, [b^{\mp 1}, b^{-l} a^{-k} b^l] \, m,$$

   so dass die Behauptung folgt.

   (b) Schreibe a, b fuer die Erzeuger. Nach der universellen Eigenschaft setzt die Abbildung $a \mapsto (1, 0)$ und $b \mapsto (0, 1)$ zu einem Gruppenhomomorphismus $F_2 \to \mathbb{Z}^2$ fort, der nach der universellen Eigenschaft der Abelisierung eindeutig ueber F_2^{ab} faktorisiert. Der so entstandene Gruppenhomomorphismus $\phi : F_2^{\mathrm{ab}} \to \mathbb{Z}^2$ ist offensichtlich surjektiv.

   Nach Teil (a) lässt sich jedes Wort w in F_2 in die Form $a^k b^l m$ bringen, wobei m in der Kommutatorgruppe liegt und $k, l \in \mathbb{Z}$ sind. Es ist $\phi(w) = (k, l)$. Ist also $\phi(w) = 0$, dann ist also w in der Kommutatorgruppe und damit trivial in F_2^{ab} , so dass ϕ auch injektiv ist. □

2. Zeige, dass die Kommutatorgruppe von $\mathrm{Per}(n)$ gleich $\mathrm{Per}^+(n)$ ist, der Gruppe der geraden Permutationen.
   (Hinweis: Zeige, dass $\mathrm{Per}^+(n)$ von den Zykeln der Länge 3 erzeugt wird.)

   Lösung. Zei Z die Gruppe, die von allen Zykeln der Länge 3 erzeugt wird. Für einen beliebigen Zykel der Länge 3 gilt

   $$(a, b, c) = (a, b)(b, c) \qquad (*)$$

   und dieser ist also gerade, so dass $Z \subset \mathrm{Per}^+(n)$ folgt. Für die umgekehrte Inklusion, reicht es zu zeigen, dass alle Produkte von zwei Transpositionen durch Zykel der Länge drei ausgedrückt werden können. Sind die beiden Transposition nicht disjunkt, so folgt dies bereits aus $(*)$. Andernfalls rechnen wir für verschiedene $1 \leq a, b, c, d \leq n$,
   $$(a, b)(c, d) = (a, b, c)(b, c, d).$$

Damit ist $Z = \mathrm{Per}^+(n)$. Es gilt nun

$$[(a,c),(b,c)] = (a,c)(b,c)(a,c)^{-1}(b,c)^{-1} = (a,c)(b,c)(a,c)(b,c) = (a,b,c).$$

Damit folgt $\mathrm{Per}^+(n) \subset \mathrm{Per}(n)^{\mathrm{ab}}$. Da $\mathrm{Per}(n)/\mathrm{Per}^+(n) \cong \{\pm 1\}$ abelsch ist, folgt die umgekehrte Inklusion. □

3. Zeige, dass eine Gruppe der Ordnung 40 nicht einfach ist.

   Lösung. Die Gruppenordnung ist $40 = 2^3\,5$. Sei s die Anzahl der 5-Sylowgruppen, dann ist $s \equiv 1(5)$, also $s \in \{1, 6, 11, 16, \dots\}$ und $s|40$, also $s \in \{1, 2, 4, 8, 5, 10, 20, 40\}$. Damit folgt $s = 1$, es gibt also nur eine Untergruppe der Orndung 5 und diese muss daher normal sein. □

4. (a) Bestimme alle kommutativen Ringe mit Eins, die den Nullring (als Ring mit Eins) als Unterring haben.

   (b) Zeige, dass der Ring $\mathbb{Z}[\sqrt{3}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{3} \subset \mathbb{R}$ unendlich viele Einheiten hat.

   Lösung. (a) Sei R ein solcher Ring. Da $0 = 1$ in R, gilt für beliebiges $x \in R$, dass

   $$x = 1 \cdot x = 0 \cdots x = 0.$$

   Also ist R schon der Nullring.

   (b) Es gilt $(\sqrt{3}+2)(\sqrt{3}-2) = 9 - 8 = 1$. Daher ist $2+\sqrt{3}$ eine Einheit. Ihr Betrag ist $|2+\sqrt{3}| = \sqrt{4+9} = \sqrt{13} > 1$. Damit kann diese Zahl in der Gruppe $\mathbb{C}^\times$ keine endliche Ordnung haben. □

Blatt 5

1. Sei $R \neq \{0\}$ ein kommutativer Ring mit Eins und fuer $x \in R$ sei $L_x : R \to R$ die Abbildung $y \mapsto xy$. Zeige

   (a) R ist genau dann ein Integritaetsring wenn L_x fuer jedes $x \neq 0$ injektiv ist.

   (b) R ist genau dann ein Koerper, wenn L_x fuer jedes $x \neq 0$ surjektiv ist.

   Lösung. (a) "⇒" Sei R ein Integritaetsring und seien $x \neq 0$ in R, sowie $y, z \in R$ mit $L_x(y) = L_x(z)$, also $x(y-z) = 0$, da $x \neq 0$ folgt $y - z = 0$ also ist L_x injektiv. "⇐" Seien $x, y \neq 0$ in R. Es gilt $L_x(0) = x0 = 0$ und da L_x injektiv ist, folgt $xy = L_x(y) \neq 0$ und damit ist R integer.

   (b) Sei R ein Koerper. Dann gilt fuer $x \neq 0$, dass $L_{x^{-1}} = L_x^{-1}$ und daher ist L_x invertierbar, also surjektiv. Ist umgekehrt L_x surjektiv, dann gibe es $y \in R$ mit $xy = L_x(y) = 1$ und daher ist x invertierbar, R also ein Koerper. □

2. Gibt es einen Integritaetsring mit genau 10 Elementen?

   Lösung. Nein. Sei R ein Ring mit 10 Elementen. In der additiven Gruppe von R gibt es eine 2-Sylow-Gruppe, also ein Element α der Ordnung 2. Ebenso gibt es ein Element β der Ordnung 5. Sei n die Ordnung des Elementes 1. Dann folgt $0 = n1\alpha = n\alpha$, also ist n ein Vielfaches von 2. Ebenso ist $n\beta = 0$, also ist n ein Vielfaches von 5. Damit muss $n = 10$ sein, die Gruppe also zyklisch und daher sind 2 und 5 ungleich Null, aber $2 \cdot 5 = 0$. Daher ist R kein Integritätsring. □

3. Sei K ein Körper. Wir identifizieren die Menge aller Folgen $(f_j)_{j \geq 0}$ in K mit der Menge aller *formalen Potenzreihen*

$$K[[x]] := \left\{ \sum_{n=0}^{\infty} f_n \, x^n : f_j \in K \right\}.$$

   Wir definieren eine Addition

$$\left(\sum_{n=0}^{\infty} a_n \, x^n \right) + \left(\sum_{n=0}^{\infty} b_n \, x^n \right) := \sum_{n=0}^{\infty} (a_n + b_n) \, x^n$$

   und Multiplikation

$$\left(\sum_{n=0}^{\infty} a_n \, x^n \right) \left(\sum_{n=0}^{\infty} b_n \, x^n \right) := \sum_{n=0}^{\infty} c_n \, x^n$$

   mit $c_n = \sum_{j=0}^{n} a_j \, b_{n-j}$.

   (a) Zeige, dass $K[[x]]$ mit diesen Verknüpfungen ein kommutativer Ring mit Eins ist.

(b) Zeige, dass $f(x) = \sum_{n=0}^{\infty} f_n\, x^n$ genau dann eine Einheit ist, wenn $f_0 \neq 0$.

Lösung. (a) Nachrechnen.

(b) Sei $a = \sum_{n=0}^{\infty} a_n x^n$ eine Einheit, dann gibt es $b = \sum_{n=0}^{\infty} b_n x^n$ mit $ab = 1$. Damit ist

$$1 = ab = a_0 b_0 + x f(x)$$

fuer eine Potenzreihe f. Es folgt $a_0 b_0 = 1$, also $a_0 \neq 0$.

Umgekehrt gelte $a_0 \neq 0$. Wir betrachten $a = \sum_{n=0}^{\infty} a_n x^n$ als gegeben und betrachten

$$1 = ab = \left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} x^n \left(\sum_{k=0}^{n} a_k b_{n-k}\right)$$

als Gleichungssystem mit den Unbekannten b_j. Zunaechst ist $a_0 b_0 = 1$, also $b_0 = a_0^{-1}$. Als naechstes gilt $a_0 b_1 + a_1 b_0 = 0$, also $b_1 = -\frac{a_1 b_0}{a_0}$. Nehmen wir induktiv an, wir haben die eindeutige Loesung $b_0, b_1, \ldots, b_n$ gefunden. Dann ist $0 = \sum_{k=0}^{n+1} a_k b_{n+1-k}$, also ist $b_{n+1} = -\frac{1}{a_0} \sum_{j=0}^{n} a_k b_{n-k}$. Die eindeutige Loesung fuer $n+1$. Induktiv erhalten wir eine eindeutige Loesung b_{n+1}. □

4. Zeige, dass der Ring $R = K[[x]]$ der formalen Potenzreihen über einem Körper K ein Hauptidealring ist.

Lösung. In der Tat gibt es nur die Ideale 0 und $x^n R$ mit $n \in \mathbb{N}_0$. Zum Beweis sei I ein Ideal $\neq 0$. Dann gibt es ein $f \in I$ mit $f = \sum_{j=n}^{\infty} f_j x^j$ mit minimalem n, so dass $f_n \neq 0$. Dann ist $f = x^n h(x)$ mit einer Einheit $h(x)$, also ist $fR = x^n R \subset I$. da aber n minimal war, liegt jedes Element von I schon in $x^n R$. □

Blatt 6

1. Sei R ein Ring und $I \subset R$ ein Ideal mit der Eigenschaft $\bigcap_{k\in\mathbb{N}} I^k = \{0\}$. Wir schreiben $I^0 = R$. Für $x \neq y$ in R sei

$$v(x,y) \coloneqq \max\{k \in \mathbb{N}_0 : x - y \in I^k\}.$$

Zeige, dass

$$d(x,y) \coloneqq \begin{cases} e^{-v(x,y)} & x \neq y, \\ 0 & x = y, \end{cases}$$

eine Metrik auf R definiert. Zeige, dass diese Metrik sogar die *starke Dreiecksungleichung* erfüllt:

$$d(x,y) \leq \max\Big(d(x,z), d(z,y)\Big), \quad x,y,z \in R.$$

Folgere, dass jeder Punkt eines Balls $B_r(a) = \{x \in R : d(x,a) < r\}$, $a \in R$, $r > 0$ ein Mittelpunkt ist. (Man nennt d die *I-adische Metrik*.)

Lösung. Nach Definition gilt $d(x,y) = d(y,x) \geq 0$ und $d(x,y) = 0 \Leftrightarrow x = y$. Daher ist nur die Dreiecksungleichung zu zeigen. Diese folgt aus der starken Dreiecksungleichung. Wir können $x,y,z \in R$ als verschieden annehmen. Gilt $x - z \in I^k$ und $z - y \in I^l$, dann folgt $x - y = (x - z) + (z - y) \in I^{\min(k,l)}$ und daher

$$v(x,y) \geq \min\Big(v(x,z), v(z,y)\Big),$$

was, da $t \mapsto e^{-t}$ streng monoton fallend ist, gleichbedeutend zu $d(x,y) \leq \max\Big(d(x,z), d(z,y)\Big)$ ist. Daher ist d eine Metrik.

Liegt $b \in B_r(a)$ und ist $x \in B_r(a)$ beliebig, dann gilt

$$d(b,x) \leq \max\Big(d(b,a), d(a,x)\Big) < r,$$

also folgt $B_r(a) \subset B_r(b)$ und da auch $a \in B_r(b)$ folgt Gleichheit. □

2. (a) Zeige, dass ein Polynom $ax^2 + bx + c$ vom Grad 2 ueber einem Koerper K mit $\mathrm{Char}(K) \neq 2$ genau dann irreduzibel ist, wenn $b^2 - 4ac$ kein Quadrat in K ist.

   (b) Zeige, dass $3x^2 + 4x + 3$ als Polynom ueber $\mathbb{Z}\left[\sqrt{-5}\right]$ irreduzibel, ueber $\mathbb{Q}\left[\sqrt{-5}\right]$ aber reduzibel ist.

Lösung. (a) Das Polynom $p(x) = ax^2 + bx + c$ mit $a \neq 0$ ist genau dann reduzibel, wenn es in Linearfaktoren zerfällt, also von der Form $a(x - \lambda_1)(x - \lambda_2)$ ist. Laut Mitternachtsformel gilt dann

$$\lambda_j = \frac{1}{2a}\left(b \pm \sqrt{b^2 - 4ac}\right),$$

falls diese Wurzel in K existiert, also $b^2 - 4ac$ ein Quadrat ist. Umgekehrt sichert die Mitternachtsformel auch die Existenz dieser Wurzel, falls

$p(x)$ eine Nullstelle hat, also reduzibel ist, womit die verlangte Aequivalenz bewiesen ist.

(b) Die komplexen Nullstellen dieses Polynoms sind

$$\frac{1}{6}\left(4 \pm \sqrt{16 - 4 \cdot 9}\right) = \frac{1}{6}\left(4 \pm 2\sqrt{4 - 9}\right) = \frac{1}{6}\left(4 \pm 2\sqrt{-5}\right).$$

Diese liegen in $\mathbb{Q}[\sqrt{-5}]$, aber nicht in $\mathbb{Z}[\sqrt{-5}]$. □

3. Sei $\phi : \mathbb{R} \to \mathbb{R}$ ein Automorphismus. Zeige, dass $\phi = \mathrm{Id}_{\mathbb{R}}$.

   Lösung. Zunächst zeigen wir, dass $\phi|_{\mathbb{Q}} = \mathrm{Id}$: Da ϕ ein additiver Gruppenhomomorphismus ist, folgt $\phi(kx) = k\phi(x)$ für $x \in \mathbb{Q}$ und $k \in \mathbb{Z}$. Da $\phi(1) = 1$, ist also $\phi|_{\mathbb{Z}} = \mathrm{Id}$. Ist $\frac{p}{q} \in \mathbb{Q}$, dann gilt

   $$\phi\left(\frac{p}{q}\right) = \frac{q}{q}\phi\left(\frac{p}{q}\right) = \frac{1}{q}\phi(p) = \frac{p}{q},$$

   also, wie verlangt, $\phi|_{\mathbb{Q}} = \mathrm{Id}$.

   Wir nutzen nun aus, dass die positiven Elemente in $\mathbb{R}$ genau die Quadrate sind. Der Homomorphismus ϕ wirft Quadrate auf Quadrate, dasselbe tut ϕ^{-1}, also $x > 0 \Leftrightarrow \phi(x) > 0$. Fuer $x, y \in \mathbb{R}$ folgt dann

   $$x < y \quad \Leftrightarrow \quad 0 < y - x \Leftrightarrow \quad 0 < \phi(y) - \phi(x) \quad \Leftrightarrow \quad \phi(x) < \phi(y).$$

   Damit erhalten ϕ und ϕ^{-1} die Anordnung, ϕ^{-1} wirft also offene Intervalle auf offene Intervalle und damit auch offene Mengen auf offene Mengen, d.h., ϕ ist stetig. Auf $\mathbb{Q}$ ist ϕ die Identitaet und da $\mathbb{Q}$ dicht liegt in $\mathbb{R}$, ist $\phi = \mathrm{Id}_{\mathbb{R}}$. □

4. Seien K ein Koerper, $n \in \mathbb{N}$ und sei $\rho_K(n)$ die maximale Dimension eines Unterraums $V \subset \mathrm{M}_n(K)$, der ausser Null nur invertierbare Matrizen enthaelt.

   Zeige

   (a) $\rho_K(n) \leq n$,

   (b) $\rho_K(n) = 1$, falls K algebraisch abgeschlossen ist,

   (c) $\rho_{\mathbb{Q}}(n) = n$.

   Lösung. (a) Seien $A_1, \ldots, A_{n+1} \in \mathrm{M}_n(K)$ linear unabhaengig und seien $v_1, \ldots, v_{n+1}$ deren erste Spalten. Diese sind linear abhaengig, also gibt es $\lambda_1, \ldots, \lambda_{n+1} \in K$, nicht alle Null, so dass $0 \neq A = \lambda_1 A_1 + \cdots + \lambda_{n+1} A_{n+1}$ erste Spalte Null, also Determinante Null hat.

   (b) Sei $K = \overline{K}$ und nimm an, es gibt $A, B \in \mathrm{M}_n(K)$ linear unabhaengig, so dass jede Matrix der Form $\lambda A + \mu B$ mit $(\lambda, \mu) \neq (0, 0)$, invertierbar ist. Das Polynom $P(x) = \det(xA + B) = \det(A)\det(x + A^{-1}B)$ ist nicht konstant, hat also eine Nullstelle x_0. Nach Voraussetzung muss aber $x_0 A + B$ invertierbar oder Null sein, also folgt $x_0 A + B = 0$, was der Linearen Unabhaengigkeit widerspricht!

(c) Sei p eine Primzahl. Nach dem Eisenstein-Kriterium ist $f(x) = x^n - p$ irreduzibel und daher ist $L = \mathbb{Q}[x]/f\mathbb{Q}[x]$ eine Koerpererweiterung von $\mathbb{Q}$ vom Grad n. Sei $v_1, \ldots, v_n$ eine Basis von L ueber $\mathbb{Q}$. Fuer $\lambda \in L$ sei $A(\lambda)$ die Matrix der Abbildung $x \mapsto \lambda x$ und sei $V \subset \mathrm{M}_n(K)$ der Raum aller $A(\lambda)$. Da L ein Koerper ist, sind alle $A(\lambda)$, die nicht Null sind, invertierbar. Da $\dim V = [L : K] = n$ folgt die Behauptung. □

Blatt 7

1. (a) Sei $n \geq 2$ eine natürliche Zahl. Gibt es eine Körpererweiterung von Grad n?

   (b) Seien K ein Körper, R/K eine Ringerweiterung von endlichem Grad. Zeige: ist R integer, dann ist R ein Körper.

   Lösung. (a) Das Polynom $f(x) = x^n - 2$ in $\mathbb{Z}[x]$ ist nach Eisenstein irreduzibel, also ist $K = \mathbb{Q}[x]/f\mathbb{Q}[x]$ eine Körpererweiterung vom Grad n.

   (b) Sei $a \in R$. Da R integer ist, ist die K-lineare Abbildung $M_a : R \to R$, $x \mapsto ax$ injektiv, also auch surjektiv, da R endlich-dimensional ueber K ist. Damit existiert ein $b \in R$ mit $ab = 1$ und a ist invertierbar. □

2. Seien $f, g \in K[x]$ normierte Polynome über einem Körper K und sei $n \in \mathbb{N}$, so dass $f^n = g^n$. Zeige, dass $f = h$.

   Lösung. Sei $P \subset K[x]$ ein Vertretersystem aller Primelemente modulo Assoziiertheit. Seien $f = u \prod_{p \in P} p^{v_p(f)}$ und $g = v \prod_{p \in P} p^{v_p(g)}$ die Primfaktorzerlegungen, wobei u, v Einheiten sind. Dann folgt

   $$u^n \prod_{p \in P} p^{nv_p(f)} = f^n = g^n = v^n \prod_{p \in P} p^{nv_p(g)}.$$

   Wegen der Eindeutigkeit der Primfaktorzerlegung folgt $nv_p(a) = nv_p(b)$ fuer jedes $p \in P$, also $v_p(a) = v_p(b)$ und daher

   $$f = u \prod_{p \in P} p^{v_p(f)} = \frac{u}{v} v \prod_{p \in P} p^{v_p(g)} = \frac{u}{v} g$$

   und da f und g normiert sind, folgt $\frac{u}{v} = 1$. □

3. Sei $f \in K[x]$ irreduzibel und sei L/K eine Koerperweiterung, die eine Nullstelle α von f enthaelt. Zeige:

   $$f'(\alpha) = 0 \quad \Leftrightarrow \quad f' = 0.$$

   Folgere: Ist α eine mehrfache Nullstelle, dann sind alle Nullstellen mehrfach.

   Lösung. Wir koennen $f \neq 0$ und $L = K[x]/f(x)$ voraussetzen. Da x die Rolle von α uebernimmt, folgt aus $f'(\alpha) = 0$ schon, dass $f'(x)$ in $K[x]$ ein Vielfaches von $f(x)$ sein muss. Da der Grad von f' aber kleiner ist als der von f, folgt $f' = 0$. Die Folgerung ist klar, da dann jede Nullstelle eine Nullstelle von f' ist. □

4. Sei R ein kommutativer Ring mit Eins. Zeige die Aequivalenz der folgenden Aussagen:

   (a) Jede aufsteigende Folge $I_1 \subset I_2 \subset \ldots$ von Idealen wird stationaer, d.h., es gibt ein j_0 mit $I_j = I_{j_0}$ fuer jedes $j \geq j_0$.

   (b) Jede nichtleere Menge M von Idealen enthaelt ein maximales Element.

(c) Jedes Ideal ist endlich erzeugt.

Einen Ring, der diese Eigenschaft hat, nennt man einen *noetherschen Ring*. Hauptidealringe sind zB noethersch.

Lösung. (a)⇒(b): Sei $I_1 \in M$ irgendein Ideal. Ist I_1 maximal, haben wir gewonnen. Andernfalls gibt es ein Ideal $I_1 \subsetneq I_2 \in M$. Ist dieses maximal, wieder Bingo, sonst machen wir weiter und erhalten eine aufsteigende Kette $I_1 \subset I_2 \subset \ldots$ von Idealen, diese muss stationär werden, was nur bedeuten kann, dass der Algorithmus abbricht, d.h., wir haben ein maximales Ideal gefunden.

(b)⇒(c): Sei I ein Ideal und M die Menge aller endlich erzeugten Unterideale von I. Darin gibt es dann ein maximales, nennen wir es J. Wir behaupten, dass $J = I$ ist. Angenommen, dies ist nicht der Fall. Seien dann $a_1, \ldots, a_n$ Erzeuger von J. Ist $J \neq I$, dann gibt es ein $a_{n+1} \in I \setminus J$ und dann ist $J' = \langle a_1, \ldots, a_n, a_{n+1} \rangle$ ein endlich erzeugtes Unterideal von I mit $J \subsetneq J'$, also war J nicht maximal, Widerspruch!

(c)⇒(a): Sei $I_1 \subset I_2 \subset \ldots$ eine Folge von Idealen und sei $I = \bigcup_{n=1}^{\infty} I_n$. Dann ist I ein Ideal und daher endlich erzeugt. Sei $E \subset I$ eine endliche Erzeugermenge. Fuer jedes $e \in E$ gibt es ein $n(e) \in \mathbb{N}$ so dass $e \in I_n$. Sei k das Maximum dieser endlich vielen Zahlen $n(e)$, $e \in E$. Dann folgt $E \subset I_k$ und damit $I_k = I$, also ist die Folge ab diesem k stationär. □

Blatt 8

1. Zeige, dass es keinen Ringhomomorphismus von $\mathbb{Q}(i)$ nach $\mathbb{Q}(\sqrt{2})$ gibt.

   Lösung. Der Körper $\mathbb{Q}(\sqrt{2})$ ist ein Unterkörper von $\mathbb{R}$, enthält also keine Lösung für die Gleichung $x^2 + 1 = 0$. Gäbe es aber einen Ringhomomorphismus $\phi : \mathbb{Q}(i) \to \mathbb{Q}(\sqrt{2})$, dann gölte

   $$\phi(i)^2 + 1 = \phi(i^2 + 1) = 0.$$

   Widerspruch! □

2. Sei L/K eine Koerpererweiterung, deren Grad eine Primzahl p ist. Zeige, dass $L = K(\alpha)$ fuer jedes $\alpha \in L \setminus K$.

   Lösung. Sei $\alpha \in L \setminus K$ und sei $M = K(\alpha)$. Wir wollen zeigen, dass $M = L$ ist. Nach der Gradformel gilt $p = [L : K] = [L : M][M : K]$ und das $M \neq K$, also $[M : K] > 1$, sowie p eine Primzahl ist, folgt $[L : M] = 1$, also $M = L$. □

3. Sei L/K eine algebraische Erweiterung so dass jedes $f \in K[x]$ ueber L in Linearfaktoren zerfaellt. Zeige dass L ein algebraischer Abschluss von K ist.

   Lösung. Sei $\overline{L}$ ein algebraischer Abschluss von L. Dann ist $\overline{L}/K$ algebraisch. Sei also $\alpha \in \overline{L}$ und $m(x) \in K[x]$ sein Minimalpolynom. Dann ist $m(x) = (x - \lambda_1) \cdots (x - \lambda_n)$ mit $\lambda_1, \ldots, \lambda_n \in L$. Dann mus α eines der λ_j sein, also ist $\alpha \in L$ und damit $L = \overline{L}$. □

4. Sei L/K eine algebraische Erweiterung und M ein Zwischenkörper. Dann gilt

   $$L/K \text{ normal} \quad \Rightarrow \quad L/M \text{ normal}.$$

   Lösung. Seien $\sigma, \sigma' : L \to \overline{M}$ Homomorphismen über M, also $\sigma|_M = \mathrm{Id}$ und ebenso für σ'. Da M/K algebraisch ist, ist $\overline{M} = \overline{K}$ und σ, σ' sind ebenfalls K-Homomorphismen und haben daher dasselbe Bild. □

Blatt 9

1. Eine Zahl $\alpha \in \overline{\mathbb{Q}}$ heisst *total reell*, falls $\sigma(\alpha) \in \mathbb{R}$ fu4r jede Einbettung $\sigma : \overline{\mathbb{Q}} \to \mathbb{C}$ gilt.

   Sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ total reell. Es gebe ein $m \in \mathbb{N}$ mit $\alpha^m \in \mathbb{Q}$. Zeige, dass $\mathbb{Q}(\alpha)$ vom Grad 2 ist und $m = 2$.

   Lösung. Seien $\alpha_1, \dots \alpha_n$ die Konjugierten zu α. Wegen $\alpha^m \in \mathbb{Q}$ folgt $\alpha^m = \alpha_j^m$ fuer jedes j, also $\alpha_j/\alpha)^m = 1$. Da aber $\alpha_j/\alpha \in \mathbb{R}$, folgt $\alpha_j/\alpha = \pm 1$. □

2. Sei K ein Koerper. Sei L/K eine algebraische Koerpererweiterung. Sei L^{sep} die Menge aller separablen Elemente in L.

   Zeige, dass L^{sep} ein Zwischenkoerper ist und dass L^{sep}/K eine separable Erweiterung ist. Zeige ferner, dass L/L^{sep} eine *rein inseparable* Erweiterung ist, d.h., kein Element fon $L \setminus L^{\text{sep}}$ ist separabel ueber L^{sep}.

   Lösung. L^{sep} ist ein Körper, denn mit $a, b \in L^{\text{sep}}$ ist $K(a, b)$ separabel über K und damit liegen $a + b, ab$ und $a^{-1}, a \neq 0$ in L^{sep}. Aus demselben Grund ist L^{sep}/K separabel.

   Ist $\alpha \in L$ separabel ueber L^{sep} und sei $m(x) = a_1 + \cdots + a_n x^n$ das MiPo in L^{sep}. Dann ist α separabel ueber $K(a_1, \dots, a_n)$ und damit ueber K, also $\alpha \in L^{\text{sep}}$. □

3. Sei L/K eine endliche Galois-Erweiterung mit Gruppe G. Seien H_1, H_2 Untergruppen und F_1, F_2 ihre Fixkoerper. Zeige, dass fuer $\sigma \in G$ gilt
$$\sigma(F_1) = F_2 \quad \Leftrightarrow \quad H_2 = \sigma H_1 \sigma^{-1}.$$

   Lösung. Sei $E = \text{Gal}(L/\sigma(F_1))$.

$$\begin{aligned} g \in H_1 &\Leftrightarrow g|_{F_1} = \text{Id} \\ &\Leftrightarrow \sigma g|_{F_1} = \sigma \\ &\Leftrightarrow \sigma g \sigma^{-1}|_{\sigma F_1} = \text{Id} \\ &\Leftrightarrow \sigma g \sigma^{-1} \in E, \end{aligned}$$

   also $E = \sigma H_1 \sigma^{-1}$.

   "$\Rightarrow$": Ist $\sigma(F_1) = F_2$, dann folgt $E = H_2$ und damit die Behauptung.

   "$\Leftarrow$": Es folgt $\text{Gal}(L/F_2) = H_2 = E = \text{Gal}(L/\sigma(F_1))$, so dass nach dem Hauptsatz der Galois-Theorie folgt $F_2 = \sigma(F_1)$. □

4. Zeige, dass $L = \mathbb{Q}\left(\sqrt[4]{2}, i\right)/\mathbb{Q}$ galoisch ist und bestimme die Struktur der Galois-Gruppe.
   (Hinweis: Die Galois-Gruppe permutiert die Nullstellen von $f(x) = x^4 - 2$.)

   Lösung. Der Körper L enthält 4 Nullstellen von $f(x)$, nämlich $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$, also zerfällt f in L in Linearfaktoren. Damit ist L der

Zerfällungskörper von f, die Erweiterung L/K also normal und daher, da separabel wegen Charakteristik Null, auch schon galoisch.

Jedes $\sigma \in G = \mathrm{Gal}(L/\mathbb{Q})$ permutiert die Nullstellen von f und ist durch diese Permutation eindeutig festgelegt, wir erhalten also eine Injektion $\Phi : G \hookrightarrow \mathrm{Per}(4)$, $\sigma \mapsto \hat{\sigma}$. Jedes σ wirft i auf $\pm i$ und da sich $\mathbb{Q}(i) \to \mathbb{Q}(i)$, $i \mapsto -i$ nach L fortsetzen lässt, treten beide Fälle auf. Sei $H \subset G$ der Stabilisator von i, dann hat H den Index $2 = [\mathbb{Q}(i) : \mathbb{Q}]$ und für $\sigma \in H$ gilt $\sigma(\pm i\alpha) = \pm i\sigma(\alpha)$ und daher ist σ durch das Bild $\sigma(\alpha) \in \{\alpha, -\alpha, i\alpha, -i\alpha\}$ eindeutig festgelegt und da $|H| = 4$, tritt jedes Element auf. Ist $\sigma(\alpha) = i\alpha$, dann folgt $\sigma^2(\alpha) = -\alpha$, also ist $\sigma^2 \neq \mathrm{Id}$ und daher hat σ die Ordnung 4 und H ist zyklisch. Der Erzeuger σ hat die Zykelschreibweise $(\alpha, i\alpha, -\alpha, -i\alpha)$

Ist nun $\tau \in G$ irgendein Element mit $\tau(i) = -i$. Dann kann durch Nachschalten eines Elementes von H erreicht werden, dass $\tau(\alpha) = \alpha$ ist. Dann hat τ die Zykelschreibweise $(i\alpha, -i\alpha)$. Hieraus folgt $\tau^2 = 1$ und $\tau\sigma\tau = \sigma^{-1}$, also ist G die Diedergruppe D_4. □

Blatt 10

1. Bestimme die Galoisgruppe Γ von $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)/\mathbb{Q}$. Gib alle Untergruppen von Γ und alle Zwischenkoerper an.

   Lösung. Wir haben die offensichtlichen Unterkoerper $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$ da alle Zwischenerweiterungen quadratisch sind, sind alle normal. Separabel sind sie wegen Charakteristik 0 sowieso. Sei nun α der Erzeuger von $\mathrm{Gal}\left(L/\mathbb{Q}(\sqrt{3})\right)$ und β der von $\mathrm{Gal}\left(L/\mathbb{Q}(\sqrt{2})\right)$. Dann ist $\alpha(\sqrt{2}) = -\sqrt{2}$ und $\alpha(\sqrt{3}) = \sqrt{3}$ und bei β ist's gerade umgekehrt. α und β haben beide Ordnung 2 und kommutieren, erzeugen also eine Untergruppe der Form $\mathbb{Z}/2 \times \mathbb{Z}/2$, das muss aus Gradgruenden schon die ganze Galoisgrupe von $L/\mathbb{Q}$ sein. Die Untergruppen sind $\langle\alpha\rangle, \langle\beta\rangle, \langle\alpha\beta\rangle$ diese korrespondieren zu den Zwischenkoerpern $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{6})$ und das sind dann alle. □

2. Eine endliche Galois-Erweiterung L/K heisst *abelsch*, falls die Galois-Gruppe $\mathrm{Gal}(L/K)$ abelsch ist. Sei $f \in K[x]$ ein separables irreduzibles Polynom und sei L der Zerfaellungskoerper. Zeige: Ist L/K abelsch, dann ist $L = K(\alpha)$ fuer jede Nullstelle $\alpha \in L$ von f.

   Lösung. Die Galois-Gruppe $\mathrm{Gal}(L/K(\alpha))$ ist normal in $\mathrm{Gal}(L/K)$ und damit ist $K(\alpha)/K$ galoisch, also normal und enthaelt demzufolge alle Nullstellen von f und daher ist $K(\alpha)$ der Zerfaellungskoerper, also L. □

3. Sei L/K eine endliche Galois-Erweiterung mit Gruppe G. Seien Γ, Σ Untergruppen und E, F ihre Fixkoerper. Zeige, dass die Erweiterung L/EF galoisch ist und druecke die Galois-Gruppe durch Γ und Σ aus.

   Lösung. Die Erweiterung ist normal und separabel, also galoisch. Wir behaupten, dass

   $$\mathrm{Gal}(L/EF) = \Gamma \cap \Sigma.$$

   Sei $\tau \in \mathrm{Gal}(L/EF)$, dann ist $\tau|_{EF} = \mathrm{Id}$, also $\tau|_E = \mathrm{Id}$ und daher $\tau \in \Gamma$. Ebenso folgt $\tau \in \Sigma$ und damit $\tau \in \Gamma \cap \Sigma$ und wir haben "$\subset$" gezeigt. Ist umgekehrt $\tau \in \Gamma \cap \Sigma$, dann liegen E und F beide im Fixkoerper von τ, also liegt auch EF im Fixkoerper von τ und damit $\tau \in \mathrm{Gal}(L/EF)$, so dass "$\supset$" folgt. □

4. Eine Galois-Erweiterung L/K heisst *zyklisch*, falls die Galois-Gruppe $\mathrm{Gal}(L/K)$ zyklisch ist. Sei Ω ein algebraisch abgeschlossener Koerper und sei $\sigma : \Omega \to \Omega$ ein Automorphismus. Sei $K = \Omega^\sigma$ der Fixkoerper von σ. Zeige, dass jede endliche Erweiterung von K eine zyklische Galois-Erweiterung ist.

   Lösung. Fuer jedes $m \in \mathbb{N}$ gilt

   $$\left(\Omega^{\sigma^m}\right)^\sigma = K$$

und daher ist Ω^{σ^m}/K galoisch mit Gruppe $\mathrm{Gal}\left(\Omega^{\sigma^m}/K\right) \cong \mathbb{Z}/n$. Wir behaupten, dass jede endliche Erweiterung L/K von der Form $L = \Omega^{\sigma^n}$ ist fuer ein $n \in \mathbb{N}$.

Sei $\widehat{L}$ die normale Huelle von L. Dann ist $\widehat{L}$ Zerfaellungskoerper eines Polynoms $f(x) \in K[x]$. Die Nullstellen von f werden von σ permutiert. Es gibt also ein $m \in \mathbb{N}$, so dass σ^m diese Nullstellen trivial permutiert, also $L \subset \widehat{L} \subset \Omega^{\sigma^m}$. Nun ist $\Omega^{\sigma^m}/K)$ zyklisch und daher ist die Untergruppe $\mathrm{Gal}(\Omega^{\sigma^m}/L)$ zyklisch und normal. Daher ist L/K galoisch und die Galois-Gruppe $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\Omega^{\sigma^m}/K)/\mathrm{Gal}(L/K)$ ist zyklisch. □

Blatt 11

1. Sei $K/\mathbb{Q}$ endlich. Zeige, dass K nur endlich viele Einheitswurzeln enthaelt.
(Hinweis: Eulers ϕ.)

   Lösung. Enthaelt K eine primitive n-te Einheitswurzel ε_n, dann folgt $\mathbb{Q}(\varepsilon_n) \subset K$ und damit $[K:\mathbb{Q}] \geq [\mathbb{Q}(\varepsilon_n):\mathbb{Q}] = \phi(n)$. Es gibt zu gegebenem $N \in \mathbb{N}$ aber nur endlich viele n mit $\phi(n) \leq N$, denn:

   Ist $\phi(n) \leq N$, dann kann keine Primzahl $> N+1$ die Zahl n teilen, da jeder Primteiler p von n einen Beitrag $p^k(p-1) \geq p-1$ liefert. Von den verbleibenden moeglichen Primzahlen p kann aber jeweils nur eine Potenz k mit $k-1 \leq \log(N)/\log(p)$ auftreten, da $p^{k-1} \leq p^{k-1}(p-1) \leq N$ gelten muss. □

2. Sei ϕ die Eulersche ϕ-Funktion.

   (a) Zeige, dass $\phi(m)\phi(n) \leq \phi(mn)$ fuer alle $m, n \in \mathbb{N}$ gilt und dass Gleichheit genau dann gilt, wenn m und n teilerfremd sind.

   (b) Zeige, dass $\phi(n) = 1 \;\Rightarrow\; n = 1, 2$.

   Lösung. (a) Fuer eine Primzahl p und $k, l \in \mathbb{N}$ gilt

$$\begin{aligned}\phi(p^k)\phi(p^l) = (p^k - p^{k-1})(p^l - p^{l-1}) &= p^{k+l} - 2p^{k+l-1} + p^{k+l-2} \\ &= p^{k+l} - p^{k+l-1} + \underbrace{p^{k+l-2}(1-p)}_{<0} \\ &< p^{k+l} - p^{k+l-1} = \phi(p^k p^l).\end{aligned}$$

   Es gilt also $\phi(p^k p^l) < \phi(p^k)\phi(p^l)$, falls k und l beide $\neq 0$ sind. Schreibe die Primfaktorzerlegungen als $m = \prod_p p^{k(p)}$ und $n = \prod_p p^{l(p)}$, wobei das Produkt formal ueber alle Primzahlen laeuft und $k(p), l(p) \in \mathbb{N}_0$ fast alle Null sind. Sei I die Menge aller Primzahlen p, fuer die $k(p) \neq 0 \neq l(p)$ gilt. Die Zahlen m und n sind genau dann teilerfremd, wenn $I = \emptyset$ gilt. In diesem Fall gilt Gleichheit laut Vorlesung. Sei nun also $I \neq \emptyset$. Wir muessen die strikte Ungleichung zeigen. Es gilt

$$\begin{aligned}\phi(m)\,\phi(n) &= \prod_{p\in I} \underbrace{\phi(p^{k(p)})\phi(p^{l(p)})}_{<\phi(p^{k(p)+l(p)})} \prod_{p\notin I} \underbrace{\phi(p^{k(p)}p^{l(p)})}_{=\phi(p^{k(p)+l(p)})} \\ &< \prod_{p\in I} \phi(p^{k(p)+l(p)}) \prod_{p\notin I} \phi(p^{k(p)+l(p)}) = \phi(mn)\end{aligned}$$

   (b) Fuer eine Primzahl p und $k \in \mathbb{N}$ gelte $\phi(p^k) = 1$, dann ist also $1 = p^{k-1}(p-1) \geq (p-1)$, so dass $p = 2$ sein muss und $k = 1$. Ist also $n = \prod_p p^{k(p)}$ mit $1 = \phi(n) = \prod_p \phi(p^{k(p)})$, dann folgt, dass alle $k(p)$ mit $p > 2$ schon gleich Null sind und $k(2) = 0, 1$ sein muss. □

3. Sei $\varepsilon = e^{2\pi i/n}$ die kanonische primitive n-te Einheitswurzel und sei $K = \mathbb{Q}(\varepsilon)$ der entsprechende Kreisteilungskoerper. Sei $\zeta \in K$ eine

Einheitswurzel beliebiger Ordnung. Zeige, dass ζ^2 eine Potenz von ε ist.

Lösung. Die Behauptung bedeutet, dass ζ^2 eine n-te Einheitswurzel ist. Zu zeigen ist also

$$\zeta^{2n} = 1.$$

Sei m die Ordnung von ζ. Die von ε und ζ erzeugte Untergruppe von $\mathbb{C}^\times$ ist zyklisch. Fixiere einen Erzeuger α. Es gilt $K = \mathbb{Q}(\varepsilon) = \mathbb{Q}(\alpha)$, denn erstens ist $\alpha \in K$ und zweitens ist ε eine Potenz von α.

Sei $k = \mathrm{ord}(\alpha)$. Dann ist n ein Teiler von k und es gilt $\zeta^k = 1$, schreibe $k = an$. Dann ist

$$\phi(n) = [\mathbb{Q}(\varepsilon) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \phi(k) = \phi(an) \geq \phi(a)\phi(n).$$

Damit ist $\phi(a) = 1$, also $a = 1, 2$. Insbesondere folgt $1 = \zeta^{2n} = 1$. □

4. Sei p eine Primzahl und sei ε eine primitive p-te Einheitswurzel. Zeige:

   (a) Die Erweiterung $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ ist zyklisch.

   (b) Es sei $p_1^{k_1} \cdots p_n^{k_n}$, $k_j \in \mathbb{N}$ die Primfaktorzerlegung von $p - 1$. Wie laesst sich die Anzahl der Zwischenkoerper $\mathbb{Q}(\varepsilon)/Z/\mathbb{Q}$ durch die p_j und k_j ausdruecken?

Lösung. (a) Die Galois-Gruppe ist $(\mathbb{Z}/p)^\times = \mathbb{F}_p^\times$ und diese Gruppe ist als Untergruppe der Einheiten eines Koerpers zyklisch.

(b) Sei Γ die Galois-Gruppe. Diese ist zyklisch und hat $p - 1$ Elemente. Daher gilt nach Chinas Restsatz

$$\Gamma \cong \mathbb{Z}/(p-1) \cong \left(\mathbb{Z}/p_1^{k_1}\right) \times \cdots \times \left(\mathbb{Z}/p_n^{k_n}\right).$$

Die Untergruppen sind genau alle Gruppen der Form

$$\prod_{i=1}^{n} \mathbb{Z}/p_i^{l_i},$$

mit $l_i = 0, 1, \ldots, k_i$. Fuer jedes i gibt es also $k_i + 1$ verschiedener Faktoren, insgesamt ist die Ordnung der Galois-Gruppe = Anzahl der Zwischenkoerper gleich

$$(k_1 + 1)(k_2 + 1) \cdots (k_n + 1).$$

□

Blatt 12

1. Zeige, dass in einem rechtwinkligen Dreieck, dessen beide kuerzeren Seitenlaengen verschiedene rationale Zahlen sind, die beiden von $\pi/2$ verschiedenen Winkel nicht in $\pi\mathbb{Q}$ liegen. (Hinweis: Wir koennen das Dreieck so drehen und verschieben, dass die Ecken in $\mathbb{C}$ gleich $0, a, a+bi$ mit $0 < a < b$ in $\mathbb{Q}$. Es gilt dann $a + bi = \sqrt{a^2+b^2}\, e^{2\pi i r}$ fuer ein $0 < r < \frac{\pi}{2}$ und wir muessen zeigen, dass $r \notin \mathbb{Q}$.)

   Lösung. **Angenommen**, $r \in \mathbb{Q}$, also $r = m/n$, dann gilt mit $\varepsilon = e^{2\pi i r}$, dass $\varepsilon^n = \left(e^{2\pi i r}\right)^n = e^{2\pi i \frac{m}{n} n} = e^{2\pi i m} = 1$. Nun ist die Einheitswurzel $\varepsilon^2 = \frac{(a+bi)^2}{a^2+b^2} \in \mathbb{Q}(i)$ und damit ist nach der letzten Aufgabe 3 Blatt 11 $\varepsilon^2 = \pm 1, \pm i$, also ist ε eine 8-te Einheitsurzel und da $0 < r < \frac{\pi}{2}$, folgt $\varepsilon = e^{2\pi i/8} = (1+i)\sqrt{2}$. Dann ist aber $a = b$. **Widerspruch!** □

2. (a) Zeige algebraisch, dass ein gleichseitiges Dreieck mit Flaecheninhalt 1 konstruierbar ist.

   (b) Gib eine geometrische Konstruktion an.

   Lösung. (a) Der Flaecheninhalt A einer gleichseitigen Dreiecks mit Grundseite g ist $A = gh/2$, wobei h de Hoehe ist. Diese erfuellt nach Pythagoras die Gleichung $h^2 + \left(\frac{g}{2}\right)^2 = g^2$, oder $h = \frac{\sqrt{3}}{2} g$, also $A = \frac{\sqrt{3}}{4} g^2$. Damit $A = 1$ wird, muss also $g = \frac{2}{\sqrt[4]{3}}$ sein. Diese liegt in der biquadratischen Erweiterung $\mathbb{Q}(\sqrt[4]{3})/\mathbb{Q}$, ist also konstruierbar.

   (b) Muehsam. □

3. Zeige, dass es auf dem Einheitskreis unendlich viele konstruierbare Punkte gibt.

   Lösung. Der Punkt 1 ist konstruierbar. Da man in $\mathcal{C}$ Wurzeln ziehen kann, ist $-1 \in \mathcal{C}$. Da man in $\mathcal{C}$ Wurzeln ziehen kann, sind $\pm i = \pm e^{2\pi/4}$ in $\mathcal{C}$. Dies iterieren wir und stellen fest, dass jede Zahl $e^{2\pi i/2^n}$, $n \in \mathbb{N}$ konstuierbar ist. □

4. Entscheide für jedes $3 \leq n \leq 16$, ob das regelmaessige n-Eck konstruierbar ist.

   Lösung. Die Konstruierbarkeit des regelmaessigen n-Ecks ist aequivalent zur Konstruierbarkeit von $\varepsilon_n = e^{2\pi i/n}$. Da Wurzeklziehen geht erhaelt man wegen der Konstruierbarkeit von $i = e^{2\pi i/4}$ die Konstruierbarkeit fuer $n = 4, 8, 16$.

   $\rho = e^{2\pi i/3}$ ist die Spitze des gleichseitigen Dreiecks mit den Ecken $0, -1, \rho$ und ein gleichseitiges Dreieck ist konstruierbar. Da Wurzelziehen geht, folgt, dass fuer $n = 3, 6, 12, 24$ die n-Ecke konstruierbar sind.

   Der Koerper $\mathbb{Q}(\varepsilon_n)$ hat Grad $\phi(n)$ ueber $\mathbb{Q}$, Daher kann ε_n nur dann konstruierbar sein, wenn $\phi(n)$ eine Zweierpotenz ist. Die Zahlen

n	7	9	11	13	14	19	21	22	23	26	28	29
$\phi(n)$	6	6	10	12	6	18	12	10	22	12	12	28

sind demnach raus.

$n = 5$: Dann ist $\phi(n) = 4$ und der Koerper $\mathbb{Q}(\varepsilon_5) \cap \mathbb{R}$ ist ein Zwischenkoerper vom Grad 2, also ist ε_5 konstruierbar. Aus demselben Grund sind ε_{10} und ε_{12} konstruierbar.

$n = 15$: Es ist $\phi(15) = 8$ und $\varepsilon_{15}^3 = \varepsilon_5$, damit enthaelt der Koerper $\mathbb{Q}(\varepsilon_{15})$ den biquadratischen Koerper $\mathbb{Q}(\varepsilon_5)$ ist ueber diesm also quadratisch und daher ist ε_{15} konstruierbar.

Konstruierbar also fuer $n = 3, 4, 5, 6, 8, 10, 12, 15, 16$

Nicht konstruierbar fuer $n = 7, 9, 11, 13, 14$ □