# Gruppentheorie

## Gruppen und Normalteiler

**Aufgabe 1**
Zeigen oder widerlegen Sie, dass die folgenden Mengen zusammen mit der angegebenen Verknüpfung Gruppen bilden:

(i) $(\mathbb{N}, \cdot)$

(ii) $(\mathbb{Z}, \oplus_k)$, wobei $m \oplus_k n = m + n + k$ für ein festes $k \in \mathbb{Z}$

(iii) $(\mathbb{Q}, -)$

(iv) $\mathrm{Sym}(X) = \{f : X \to X \mid \text{f ist bijektiv}\}$ für eine beliebige nicht-leere Menge $X$ mit der Komposition von Abbildungen

(v) $\{f_{a,b} : \mathbb{R} \to \mathbb{R}, x \mapsto ax + b \mid a, b \in \mathbb{R}\}$ mit der Komposition von Abbildungen

(vi) $\{f_{a,b} : \mathbb{R} \to \mathbb{R}, x \mapsto ax + b \mid a, b \in \mathbb{R} \text{ mit } a \neq 0\}$ mit der Komposition von Abbildungen

(vii) $(\mathcal{P}(X), \cup)$ für eine beliebige Menge $X$

(viii) $\mathrm{Mat}_2(\mathbb{R})$ mit der Matrizenmutiplikation

**Aufgabe 2**
Sei $G$ eine Gruppe. Zeigen Sie, dass eine Teilmenge $H \subset G$ genau dann eine Untergruppe von $G$ ist, wenn sie nicht leer ist und für alle $a, b \in H$ gilt, dass $ab^{-1} \in H$.

**Aufgabe 3**
Sei $G$ eine Gruppe und $N \subset G$ ein Normalteiler von $G$. Zeigen Sie, dass $N$ ein Normalteiler von jeder Untergruppe $H \subset G$ ist, welche $N$ enthält.

**Aufgabe 4**
Sei $G$ eine Gruppe und seien $N_i \subset G$, $i \in I$, eine nicht-leere Familie von normalen Untergruppen. Zeigen Sie, dass dann auch $N \subset G$ normal ist, wobei $N$ der Durchschnitt über die $N_i$, $i \in I$, ist.

**Aufgabe 5**
Sei $G$ eine endliche Gruppe. Zeigen Sie, dass jede Untergruppe $H \subset G$ mit $[G : H] = 2$ bereits ein Normalteiler ist.

**Aufgabe 6**
Sei $X$ eine endliche Menge mit $\mathrm{card}(X) \geq 4$ und $Y \subset X$ eine zweielementige Teilmenge. Zeigen Sie, dass $H = \{\sigma \in \mathrm{Sym}(X) \mid \sigma(Y) = Y\} \subset \mathrm{Sym}(X)$ eine nicht-normale Untergruppe ist.

**Aufgabe 7**
Zeigen Sie mit Hilfe folgender Anleitung, dass es eine nicht-abelsche Gruppe $G$ gibt, sodass jede Untergruppe von $G$ ein Normalteiler ist:

(i) Betrachten Sie die Untergruppe $Q_8 \subset SL_2(\mathbb{F}_3)$, welche aus den beiden Skalarmatrizen und den sechs spurlosen Matrizen besteht. Geben Sie die Elemente von $Q_8$ konkret an.

(ii) Geben Sie (nicht notwendigerweise mit ausführlicher oder formal aufgeschriebener Begründung) alle Untergruppen von $Q_8$ an.

(iii) Zeigen Sie, dass alle Untergruppen Normalteiler sind.

(iv) Zeigen Sie, dass $Q_8$ nicht abelsch ist.

Erinnerung/Hinweis: Eine Matrix, welche ein Vielfaches der Einheitsmatrix ist, nennt man Skalarmatrix; eine Matrix, bei welcher die Summe der Diagonalelemente Null ergibt, nennt man spurlos.
Tatsächlich müssen Sie für (iii) die Normalteilereigenschaft nur einmal per Hand überprüfen, wenn Sie eine geeignete Aufgabe zitieren.

## Gruppenhomomorphismen

**Aufgabe 8**
Welche der folgenden Abbildungen sind Gruppenhomomorphismen?

(i) $f : \mathbb{Z} \to \mathbb{Z}$, $m \mapsto am$ für ein festes $a \in \mathbb{Z}$

(ii) $f : \mathbb{C} \to \mathbb{R}$, $z \mapsto \|z\|$

(iii) $f : \mathbb{R} \to \mathbb{R}^\times$, $x \mapsto \exp(x)$

(iv) $f : S_3 \to S_3$, $\sigma \mapsto \sigma^{-1}$

(v) $f : \mathbb{R}[T] \to \mathbb{R}[T]$, $g \mapsto g'$

**Aufgabe 9**
Seien $G$ und $H$ Gruppen und sei $f : G \to H$ ein Gruppenhomomorphismus. Zeigen Sie, dass $f$ injektiv ist genau dann, wenn $\ker(f) = \{1\}$ gilt.

**Aufgabe 10**
Sei $\mu_4 = \{\pm 1, \pm i\} \subset \mathbb{C}^\times$ und sei $f : \mathbb{Z} \to \mu_4$, $m \mapsto i^m$. Zeigen Sie, dass $f$ ein Gruppenhomomorphismus ist und berechnen Sie $\ker(f)$. Sie müssen nicht überprüfen, dass $\mu_4$ eine Gruppe ist.

**Aufgabe 11**
Sei $G$ eine Gruppe. Zeigen Sie, dass eine Teilmenge $N \subset G$ genau dann ein Normalteiler ist, wenn es eine Gruppe $H$ und einen Gruppenhomomorphismus $f : G \to H$ mit $\ker(f) = N$ gibt.

**Aufgabe 12**
Seien $G$ und $H$ Gruppen, $N \subset G$ ein Normalteiler und $f : G \to H$ ein surjektiver Gruppenhomomorphismus. Zeigen Sie, dass $f(N) \subset H$ dann ebenfalls ein Normalteiler ist. Gilt die Aussage auch für nicht-surjektive Gruppenhomomorphismen?

**Aufgabe 13**
Seien $G$ und $H$ endliche Gruppen mit teilerfremden Ordnungen. Zeigen Sie, dass jeder Homomorphismus $f : G \to H$ trivial ist.

**Aufgabe 14**
Beschreiben Sie einen Isomorphismus $\mathrm{GL}_2(\mathbb{F}_2) \to S_3$. Beschreiben heißt hier, dass Sie erklären wie man obigen Homomorphismus definiert und begründen können, dass dieser bijektiv ist. Sie müssen nicht (zwingend) nachrechnen, dass es tatsächlich ein Homomorphismus ist.
Hinweis: Schreiben Sie sich die Gruppe $\mathrm{GL}_2(\mathbb{F}_2)$ konkret hin und wenden Sie ihre Elemente mal auf die drei Vektoren $v_i \in \mathbb{F}_2^2$, $1 \leq i \leq 3$, an, welche nicht der Nullvektor sind.

## Endlich erzeugte abelsche Gruppen

**Aufgabe 15**
Beweisen oder widerlegen Sie:

(i) Jede zyklische Gruppe ist abelsch.

(ii) Jede Untergruppe einer zyklischen Gruppe ist ein Normalteiler.

(iii) Das direkte Produkt zyklischer Gruppen ist zyklisch.

(iv) Jede Quotientengruppe einer zyklischen Gruppe ist zyklisch.

(v) Jede Gruppe von Primzahlordnung ist zyklisch.

(vi) Jede zyklische Gruppe ist von Primzahlordnung.

**Aufgabe 16**
Zeigen Sie:

(i) $\mathbb{Q}$ ist nicht zyklisch.

(ii) $\mathbb{Q}/\mathbb{Z}$ ist nicht zyklisch.

(iii) Jede endliche Teilmenge $M \subset \mathbb{Q}/\mathbb{Z}$ ist in einer zyklischen Untergruppe $H \subset \mathbb{Q}/\mathbb{Z}$ enthalten.

Hinweis: Nehmen Sie bei (ii) mal an, dass $G = \mathbb{Q}/\mathbb{Z}$ zyklisch ist und betrachten Sie zum Beispiel mal $[\frac{1}{2}] \in G$.

**Aufgabe 17**
Seien $G$ und $H$ endliche Gruppen und sei $f : G \to H$ ein Gruppenisomorphismus.

(i) Zeigen Sie, dass $\mathrm{ord}(g) = \mathrm{ord}(f(g))$ für jedes $g \in G$ gilt. Insbesondere haben also isomorphe Gruppen genau die gleiche Anzahl an Elementen einer bestimmten Ordnung.

(ii) Sei $p > 0$ eine Primzahl. Folgern Sie aus dem ersten Aufgabenteil, dass die beiden Gruppen $\mathbb{Z}/p^2\mathbb{Z}$ und $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ nicht isomorph sein können.

**Aufgabe 18**
Sei $p > 0$ eine Primzahl und $G$ eine Gruppe mit $\mathrm{ord}(G) = p^2$. Zeigen Sie mit Hilfe folgender Anleitung, dass $G$ isomorph ist zu der Gruppe $\mathbb{Z}/p^2\mathbb{Z}$ oder zu der Gruppe $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$:

(i) Sei $H$ eine beliebige Gruppe. Zeigen Sie, dass $H$ abelsch sein muss, falls $H/Z(H)$ zyklisch ist.

(ii) Machen Sie eine Fallunterscheidung anhand der Ordnung von $Z(G)$ um zu zeigen, dass $G$ abelsch ist und beenden Sie den Beweis. Dabei dürfen Sie verwenden, dass Gruppen der Ordnung $p^2$ nicht-triviales Zentrum besitzen.

(iii) Sind alle Gruppen $G$ mit $\mathrm{ord}(G) = p^n$, $n \geq 1$, abelsch?

Hinweis: Schauen Sie sich für (iii) vorherige Aufgaben an.

**Aufgabe 19**
Zeigen Sie, dass der Gruppenhomomorphismus

$$f : \mathbb{Z}/168\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}, \quad a + 168\mathbb{Z} \mapsto (a + 12\mathbb{Z}, a + 14\mathbb{Z})$$

nicht bijektiv ist. Ist $f$ bijektiv, wenn man die Zahlen $168, 12, 14$ durch $182, 13, 14$ ersetzt?

**Aufgabe 20**
Sei $G = \mathbb{Z}/1260\mathbb{Z}$. Für welche $m, n \geq 1$ gilt $G \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$?

**Aufgabe 21**
Geben Sie einen Repräsentanten für jede Isomorphieklasse abelscher Gruppen der Ordnung $538 \leq n \leq 541$ an.

## Gruppenwirkungen

**Aufgabe 22**
Sei $G$ eine Gruppe und $X$ eine nicht-leere Menge. Welche der folgenden Abbildungen $\lambda : G \times X \to X$ sind Gruppenwirkungen?

(i) $\lambda(g, x) = gxg^{-1}$, wobei $X = G$

(ii) $\lambda(g, x) = g^{-1}x$, wobei $X = G$

(iii) $\lambda(g, x) = x^{g+1}$, wobei $G = \mathbb{Z}$ und $X = \mathbb{R}^\times$

(iv) $\lambda(g, x) = x$

(v) $\lambda(A, v) = A \cdot v$, wobei $G = \mathrm{GL}_2(K)$ und $X = K^2$ für einen Körper $K$

**Aufgabe 23**
Sei $G = \mathrm{UT}_2(\mathbb{R})$ die Gruppe der oberen Dreiecksmatrizen mit Einsen auf der Diagonale und Einträgen aus $\mathbb{R}$. Bestimmen Sie die Bahnen der natürlichen Gruppenwirkung von $G$ auf $\mathbb{R}^2$ für die Elemente $0, e_1, e_1 + e_2 \in \mathbb{R}^2$, wobei $e_i \in \mathbb{R}^2$, $i = 1, 2$, die beiden Standardbasisvektoren sind.

**Aufgabe 24**
Sei $G$ eine Gruppe und $X$ eine nicht-leere Menge. Zeigen Sie, dass Gruppenwirkungen $G \times X \to X$ genau den Gruppenhomomorphismen $G \to \mathrm{Sym}(X)$

entsprechen, also zueinander inverse Bijektionen zwischen diesen beiden Mengen exisitieren.

**Aufgabe 25**
Sei $G$ eine endliche Gruppe und $H \subset G$ eine Untergruppe. Interpretieren Sie die Bahnengleichung der Gruppenwirkung $\lambda : H \times G \to G$, $(h, g) \mapsto gh$ im Sinne elementarer Gruppentheorie.
Bemerkung: Mit elementarer Gruppentheorie ist alles vor dem Abschnitt über endlich erzeugte abelsche Gruppen gemeint.

**Aufgabe 26**
Sei $G$ eine Gruppe und $X = \{H \subset G \mid H \text{ ist eine Untergruppe}\}$. Zeigen Sie, dass die Abbildung

$$\lambda : G \times X \to X, \quad (g, H) \mapsto gHg^{-1}$$

eine Gruppenwirkung ist und dann, dass eine Untergruppe $H \subset G$ ein Normalteiler ist genau dann, wenn $\mathrm{card}(G \cdot H) = 1$ gilt.

**Aufgabe 27**
Sei $G$ eine endliche Gruppe, welche transitiv auf einer Menge $X$ operiert. Zeigen Sie, dass $\mathrm{card}(X)$ ein Teiler von $\mathrm{ord}(G)$ ist.

**Aufgabe 28**
Sei $G$ eine endliche Gruppe und $p > 0$ eine Primzahl mit $p \mid \mathrm{ord}(G) = n$. Zeigen Sie mit Hilfe folgender Anleitung, dass $G$ eine Untergruppe der Ordnung $p$ besitzt:

(i) Sei $X = \{(g_1, ..., g_p) \in G^p \mid g_1 \cdot ... \cdot g_p = 1\}$ und betrachten Sie die Gruppenwirkung gegeben durch zyklische Permutation, also

$$\lambda : \mathbb{Z}/p\mathbb{Z} \times X \to X, \quad (\overline{m}, (g_1, ..., g_p)) \mapsto (g_{1+m}, ..., g_p, g_1, ..., g_m).$$

Überlegen Sie sich, dass $\lambda$ wohldefiniert ist, also $\mathrm{im}(\lambda) \subset X$ gilt.

(ii) Begründen Sie, dass $\mathrm{card}(\mathbb{Z}/p\mathbb{Z} \cdot x) = 1$ oder $\mathrm{card}(\mathbb{Z}/p\mathbb{Z} \cdot x) = p$ für jedes $x \in X$ gelten muss.

(iii) Von welcher Form muss $x \in X$ sein, wenn $\mathrm{card}(\mathbb{Z}/p\mathbb{Z} \cdot x) = 1$ gilt? Finden Sie ein Beispiel für ein solches $x \in X$.

(iv) Seien $a$ und $b$ die Anzahl der Bahnen der Kardinalität 1 bzw. $p$. Stellen Sie die Bahnengleichung in Abhängigkeit von $a$ und $b$ auf und begründen Sie, dass $\mathrm{card}(X) = n^{p-1}$ gilt.

(v) Folgern Sie, dass $p$ ein Teiler von $a$ ist und beenden Sie den Beweis.

## Permutationsgruppen

**Aufgabe 29**
Sei $G = S_6$.

(i) Geben Sie die folgenden Elemente aus $G$ in der Zykelschreibweise an:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 5 & 1 \end{pmatrix} \quad \text{und} \quad \eta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 3 & 5 \end{pmatrix}$$

(ii) Berechnen Sie $\sigma \cdot \eta^{-1}$, $\eta^2$, $\sigma^5$, $\eta^3 \cdot \sigma$ und $\eta^5$.

(iii) Bestimmen Sie das Signum der Elemente des vorherigen Aufgabenteils. Welche von diesen Elementen sind Elemente von $A_6$?

**Aufgabe 30**
Beschreiben Sie $\operatorname{ord}(S_n)$ und $\operatorname{ord}(A_n)$ für alle $n \geq 1$. Beschreiben bedeutet hier erklären, ohne es formal per Induktion zu beweisen.

**Aufgabe 31**
Sei $G$ eine Gruppe und seien $g, g' \in G$ zwei kommutierende Elemente von endlicher, teilerfremder Ordnung.

(i) Welche Ordnung hat dann $g \cdot g' \in G$?

(ii) Wie sieht die Ordnung von $g \cdot g' \in G$ konkret aus, falls die Ordnungen von $g, g' \in G$ Primzahlen sind?

(iii) Zeigen Sie, dass es in $S_{15}$ ein Element der Ordnung 105 gibt.

**Aufgabe 32**
Bestimmen Sie für jedes $n \geq 1$ das Zentrum $Z = Z(S_n) \subset S_n$.

**Aufgabe 33**
Beschreiben Sie mit Hilfe folgender Anleitung, dass $S_n$, $n \geq 3$, von zwei Elementen erzeugt wird:

(i) Erklären Sie zunächst, dass sich jeder $k$-Zykel $\sigma \in S_n$ als Produkt von $k-1$ Transpositionen $\tau_1, ..., \tau_{k-1} \in S_n$ schreiben lässt.

(ii) Begründen Sie nun, dass sich jede Transposition als Produkt von Transpositionen der Form $(k \;\; k+1)$ schreiben lässt.

(iii) Folgern Sie, dass $S_n = \langle (1 \;\; 2), (1 \;\; ... \;\; n) \rangle$.

Bemerkung: Tatsächlich gilt (iii) mit analoger Argumentation auch für eine beliebige Transposition und einen beliebigen $n$-Zykel.

**Aufgabe 34**
Betrachten Sie die Gruppe $G = S_4$.

(i) Wie sieht $V_4 = \langle (1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4) \rangle \subset G$ konkret aus?

(ii) Die Gruppe $V_4$ ist isomorph zu einer Ihnen besser geläufigen Gruppe. Welche ist das?

(iii) Zeigen Sie, dass $V_4 \subset G$ normal ist.

(iv) Geben Sie eine Kompositionsreihe von $S_4$ an. Ist $S_4$ auflösbar?

(v) Folgern Sie aus den vorherigen Aufgabenteilen, dass Normalität von Gruppen nicht transitiv ist, also Gruppen $H \subset N \subset G$ existieren, sodass $H \subset N$ und $N \subset G$ normal sind, aber $H \subset G$ nicht normal ist.

Hinweis: Sie müssen bei (iii) nicht zwingend die Normalteilerbedingung nachrechnen, wenn Sie ein geeignetes Resultat verwenden.

**Aufgabe 35**
Zeigen Sie mit Hilfe folgender Anleitung, dass es eine endliche Gruppe $G$ gibt, welche nicht zu jedem Teiler $m$ von $\mathrm{ord}(G)$ eine Untergruppe der Ordnung $m$ besitzt:

(i) Sei $G$ eine endliche Gruppe und $N \subset G$ ein Normalteiler. Sei außerdem $g \in G$ und betrachte $\overline{g} \in G/N$. Zeigen Sie, dass $\mathrm{ord}(\overline{g})$ ein Teiler von $\mathrm{ord}(g)$ ist.

(ii) Nehmen Sie nun $[G : N] = 2$ an und sei $g \in G$ von ungerader Ordnung. Zeigen Sie, dass dann $\mathrm{ord}(\overline{g}) = 1$, also $\overline{g} = \overline{1}$ gilt.

(iii) Folgern Sie, dass eine Untergruppe vom Index 2 in $A_4$ mehr als sechs Elemente beinhalten müsste und erzeugen Sie somit einen Widerspruch.

## Die Sylow-Sätze

**Aufgabe 36**
Geben Sie für die folgenden Gruppen $G$ für jeden Primteiler $p > 0$ von $\mathrm{ord}(G)$ jeweils eine Sylow-$p$-Untergruppe an:

(i) $G = \mathbb{Z}/15\mathbb{Z}$

(ii) $G = \mathrm{SL}_2(\mathbb{F}_3)$

(iii) $G = A_5$

Erinnerung/Hinweis: Die Ordnung von $\mathrm{SL}_n(\mathbb{F}_p)$ ist

$$p^{\binom{n}{2}} \prod_{i=0}^{n-2} (p^{n-i} - 1) = \frac{\prod_{i=0}^{n-1} (p^n - p^i)}{p-1},$$

wie man mit linearer Algebra durch das Zählen linear unabhängiger Vektoren zeigen kann.

**Aufgabe 37**
Sei $G$ eine endliche Gruppe und $p > 0$ ein Primteiler von $\mathrm{ord}(G)$. Angenommen, $G$ besitzt genau eine Sylow-$p$-Untergruppe $H \subset G$. Zeigen Sie, dass $H \subset G$ dann bereits ein Normalteiler sein muss.

**Aufgabe 38**
Sei $G$ eine Gruppe der Ordnung $34969 = 11^2 \cdot 17^2$. Zeigen Sie mit Hilfe folgender Anleitung, dass $G$ abelsch ist:

(i) Zeigen Sie zunächst, dass $G$ Normalteiler der Ordnung 121 und 289 besitzt.

(ii) Seien $N_1$ und $N_2$ obige Normalteiler. Zeigen Sie nun, dass $G \cong N_1 \times N_2$.

(iii) Folgern Sie, dass $G$ abelsch ist.

(iv) Gilt obige Aussage für beliebige Primzahlen $p, q > 0$?

**Aufgabe 39**
Sei $G$ eine nicht-triviale, endliche Gruppe und $p > 0$ eine Primzahl, sodass jedes Element $g \in G$ von Ordnung einer $p$-Potenz ist. Zeigen Sie mit den Sylow-Sätzen, dass dann $\mathrm{ord}(G)$ eine Potenz von $p$ ist.

**Aufgabe 40**
Klassifizieren Sie die Gruppen der Ordnung 65 bis auf Isomorphie.

**Aufgabe 41**
Sei $G$ eine nicht-zyklische Gruppe der Ordnung $51 = 3 \cdot 17$. Zeigen Sie mit dem dritten Sylow-Satz, dass $G$ genau $2 \cdot 17 = 34$ Elemente der Ordnung 3 besitzt. Was passiert bei einer nicht-zyklischen Gruppe $H$ der Ordnung $3 \cdot p$ für eine beliebige Primzahl $p > 0$? Besitzt $H$ dann $2 \cdot p$ Elemente der Ordnung 3?

**Aufgabe 42**
Sei $G$ eine endliche Gruppe der Ordnung $p^\nu \cdot m$, wobei $p$ kein Teiler von $m$ ist. Sei außerdem $N \subset G$ ein Normalteiler, sodass $p \nmid [G : N]$. Zeigen Sie mit dem zweiten Sylow-Satz, dass jede Sylow-$p$-untergruppe von $G$ in $N$ enthalten ist.

# Ringtheorie

## Ringe und Ideale

**Aufgabe 1**
Sei $R$ ein Ring und $\mathfrak{a} \subset R$ eine Teilmenge. Zeige Sie, dass $\mathfrak{a} \subset R$ ein Ideal ist genau dann, wenn $\mathfrak{a} \neq \emptyset$ und für alle $r \in R$ und alle $a, a' \in \mathfrak{a}$ gilt, dass $ra - a' \in \mathfrak{a}$.

**Aufgabe 2**
Sei $R$ ein Ring und $\mathfrak{a} \subset R$ ein Ideal.

(i) Zeigen Sie, dass $\mathfrak{a} = R$ gilt genau dann, wenn $\mathfrak{a}$ eine Einheit $u \in R^\times$ enthält.

(ii) Folgern Sie, dass die einzigen beiden Ideale eines Körpers das Nullideal und der Körper selbst sind.

**Aufgabe 3**
Sei $R$ ein Ring und seien $\mathfrak{a}, \mathfrak{b} \subset R$ Ideale. Zeigen Sie, dass die folgenden Teilmengen ebenfalls Ideale sind:

(i) $\mathfrak{a} \cap \mathfrak{b}$

(ii) $\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$

Bemerkung: Letzteres Ideal ist das von der Vereinigung von $\mathfrak{a}$ und $\mathfrak{b}$ erzeugte Ideal.

**Aufgabe 4**
Sei $R$ ein Ring und $\mathfrak{a}_i \subset R$, $i \in I$, eine nicht-leere Familie von Idealen.

(i) Angenommen, obige Familie ist totalgeordnet. Zeigen Sie, dass dann $\mathfrak{a} \subset R$ ein Ideal ist, wobei $\mathfrak{a}$ die Vereinigung über die $\mathfrak{a}_i$, $i \in I$, ist.

(ii) Geben Sie ein Beispiel dafür an, dass die Aussage ohne die zusätzliche Annahme falsch wird.

**Aufgabe 5**
Welche der folgenden Teilmengen $\mathfrak{a} \subset R$ sind Ideale?

(i) $\mathfrak{a} = 2\mathbb{Z} + 1 = \{2k + 1 \mid k \in \mathbb{Z}\}$, $R = \mathbb{Z}$

(ii) $\mathfrak{a} = 5\mathbb{Z}/15\mathbb{Z} = \{\overline{0}, \overline{5}, \overline{10}\}$, $R = \mathbb{Z}/15\mathbb{Z}$

(iii) $\mathfrak{a} = i\mathbb{Z} = \{im \mid m \in \mathbb{Z}\}$, $R = \mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}\}$

(iv) $\mathfrak{a} = i\mathbb{Z}[i] = \{im \mid m \in \mathbb{Z}[i]\}$, $R = \mathbb{Z}[i]$

(v) $\mathfrak{a} = \{\sum a_i T^i \in \mathbb{Z}[T] \mid a_0 = 4\}$, $R = \mathbb{Z}[T]$

(vi) $\mathfrak{a} = \{f \in \mathcal{C}(\mathbb{R}) \mid f(x) = 0\}$, $R = \mathcal{C}(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{C} \mid \text{f ist stetig}\}$ und $x \in \mathbb{R}$ fest

**Aufgabe 6**
Seien $R$ und $S$ Ringe und sei $\mathfrak{a} \subset R \times S$ ein Ideal. Zeigen Sie, dass es Ideale $\mathfrak{b} \subset R$, $\mathfrak{c} \subset S$ gibt, sodass $\mathfrak{a} = \mathfrak{b} \times \mathfrak{c}$ gilt.
Hinweis: Betrachten Sie $\mathfrak{b} = \{b \in R \mid \text{Es existiert ein } s \in S \text{ mit } (b,s) \in \mathfrak{a}\}$ und $\mathfrak{c} = \{c \in S \mid \text{Es existiert ein } r \in R \text{ mit } (r,c) \in \mathfrak{a}\}$

**Aufgabe 7**
Sei $R$ ein Ring. Zeigen Sie, dass die Teilmenge der nilpotenten Elemente $\mathrm{Nil}(R) = \sqrt{(0)} = \{r \in R \mid r \text{ ist nilpotent}\}$ ein Ideal von $R$ bildet. Dabei nennt man ein Element $r \in R$ nilpotent, falls eine natürliche Zahl $n \geq 1$ existiert, sodass $r^n = 0$ gilt.

## Ringhomomorphismen

**Aufgabe 8**
Sei $R$ ein Ring. Welche der folgenden Abbildungen sind Ringhomomorphismen?

(i) $f : \{0\} \to R$, $0 \mapsto 0$

(ii) $f : R \to \{0\}$, $r \mapsto 0$

(iii) $f : R \to R$, $r \mapsto -r$

(iv) $f : \mathbb{Z} \to R$, $m \mapsto m \cdot 1$

(v) $f : R \to R \times R$, $r \mapsto (r,r)$

**Aufgabe 9**
Sei $\varphi : R \to S$ ein Ringhomomophismus.

(i) Zeigen Sie, dass $\psi : R[T] \to S[T]$, $\sum a_i T^i \mapsto \sum \varphi(a_i) T^i$ dann ebenfalls ein Ringhomomorphismus ist.

(ii) Folgern Sie, dass es einen Ringhomomorphismus $\mathbb{Z}[T] \to \mathbb{F}_p[T]$ gibt.

**Aufgabe 10**
Sei $R$ ein Ring mit $R \neq \{0\}$, $K$ ein Körper und $f : K \to R$ ein Ringhomomorphismus. Zeigen Sie, dass $f$ injektiv ist. Insbesondere ist also jeder Ringhomomorphismus zwischen Körpern injektiv.

**Aufgabe 11**
Zeigen Sie, dass es genau einen Ringhomomorphismus $f : \mathbb{Z} \to R$ gibt, wobei $R$ ein beliebiger Ring ist.

**Aufgabe 12**
Sei $R$ ein Ring und seien $f, g : \mathbb{Q} \to R$ Ringhomomorphismen, sodass $f \circ i = g \circ i$ gilt, wobei $i : \mathbb{Z} \to \mathbb{Q}$ die Inklusion ist. Zeigen Sie, dass dann schon $f = g$ gelten muss.

**Aufgabe 13**
Zeigen oder widerlegen Sie:

(i) Bilder von Idealen unter Ringhomomorphismen sind Ideale.

(ii) Urbilder von Idealen unter Ringhomomorphismen sind Ideale.

(iii) Bilder von maximalen Idealen unter Ringhomomorphismen sind maximale Ideale.

(iv) Urbilder von maximalen Idealen unter Ringhomomorphismen sind maximale Ideale.

**Aufgabe 14**
Zeigen Sie den dritten Isomorphiesatz für Ringe:
Sei $R$ ein Ring und seien $\mathfrak{a}, \mathfrak{b} \subset R$ Ideale mit $\mathfrak{b} \subset \mathfrak{a}$. Dann gilt

$$(R/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b}) \cong R/\mathfrak{a}.$$

(i) Zeigen Sie zunächst, dass $\mathfrak{a}/\mathfrak{b} \subset R/\mathfrak{b}$ ein Ideal ist.

(ii) Betrachten Sie die Abbildung $\varphi : R/\mathfrak{b} \to R/\mathfrak{a}$, $r + \mathfrak{b} \mapsto r + \mathfrak{a}$ und zeigen Sie, dass $\varphi$ ein wohldefinierter, surjektiver Ringhomomorphismus ist.

(iii) Berechnen Sie den Kern von $\varphi$ und wenden Sie den ersten Isomorphiesatz an.

## Integre und faktorielle Ringe

**Aufgabe 15**
Zeigen Sie, dass Körper integer sind.

**Aufgabe 16**
Bestimmen Sie alle $n \in \mathbb{N}$, sodass $\mathbb{Z}/n\mathbb{Z}$ integer ist.

**Aufgabe 17**
Beweisen oder widerlegen Sie:

(i) Jeder Unterring eines integren Ringes ist integer.

(ii) Das direkte Produkt integrer Ringer ist integer.

(iii) Jeder Quotientenring eines integren Ringes ist integer.

(iv) Jeder integre Ring ist isomorph zu einem Unterring eines Körpers.

**Aufgabe 18**
Sei $R$ ein Ring. Ein Ideal $\mathfrak{p} \subsetneq R$ heißt Primideal, falls für alle $a, b \in R$ mit $ab \in \mathfrak{p}$ folgt, dass $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Zeigen Sie, dass ein Ideal $\mathfrak{p} \subsetneq R$ genau dann prim ist, wenn $R/\mathfrak{p}$ ein integrer Ring ist.

**Aufgabe 19**
Zeigen Sie, dass ein Ring $R$ integer ist genau dann, wenn die Multiplikation $m_a : R \to R,\ \ r \mapsto ar$ injektiv ist für alle $a \in R$ mit $a \neq 0$.

**Aufgabe 20**
Sei $R$ ein faktorieller Ring und seien $a, b \in R$ mit $a, b \neq 0$. Zeigen Sie, dass es $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ in $R$ gibt.

**Aufgabe 21**
Zeigen Sie, dass $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ nicht faktoriell ist, indem Sie verwenden, dass die Abbildung $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}$, $a + b\sqrt{-5} \mapsto a^2 + 5b^2$ multiplikativ ist.

## Hauptidealringe und euklidische Ringe

**Aufgabe 22**
Geben Sie für die folgenden Ideale $\mathfrak{a} \subset R$ ein Element $r \in R$ an, sodass $\mathfrak{a} = (r)$, falls ein solcher Erzeuger existiert oder begründen Sie, dass kein solcher Erzeuger existieren kann:

(i) $\mathfrak{a} = (4, 6)$, $R = \mathbb{Z}$

(ii) $\mathfrak{a} = (3, 29)$, $R = \mathbb{Z}[T]$

(iii) $\mathfrak{a} = (7, T)$, $R = \mathbb{Z}[i][T]$

(iv) $\mathfrak{a} = (\frac{TS^2+1,}{T}, i)$, $R = \mathbb{C}(T)[S]$

**Aufgabe 23**
Sei $R$ ein Ring, sodass $R[T]$ ein Hauptidealring ist. Zeigen Sie, dass $R$ dann bereits ein Körper ist.
Hinweis: Betrachten Sie für ein $r \in R$ mit $r \neq 0$ das Ideal $(r, T) \subset R[T]$ und verwenden Sie die Additivität des Grades von Polynomen. Zudem könnte die Evaluationsabbildung nützlich sein.

**Aufgabe 24**
Sei $K$ ein Körper. Zeigen Sie, dass $K[T_1, ..., T_n]$ für $n \geq 2$ kein Hauptidealring ist, indem Sie die vorherige Aufgabe verwenden.

**Aufgabe 25**
Zeigen Sie, dass Körper euklidisch sind.

**Aufgabe 26**
Sei $R$ ein euklidischer Ring mit euklidischer Funktion $\varphi : R \to \mathbb{N}$ und $\mathfrak{a} \subset R$ ein Ideal. Zeigen Sie, dass $R$ ein Hauptidealring ist, indem Sie zunächst den Fall des Nullideals betrachten und anschließend zeigen, dass $a \neq 0$ in $\mathfrak{a}$ mit $\varphi(a) \in \mathbb{N}$ minimal ein Erzeuger von $\mathfrak{a}$ ist.

**Aufgabe 27**
Sei $R$ ein integrer Ring und $F = \mathrm{Frac}(R)$. Angenommen, es existiert eine Abbildung $\nu : F \to \mathbb{Z} \cup \{\infty\}$ mit $\nu(ab) = \nu(a) + \nu(b)$ für alle $a, b \in F$, sodass $R = \{a \in F \mid \nu(a) \geq 0\}$. Zeigen Sie, dass $R$ euklidisch ist mit euklidischer Funktion $\varphi : R \setminus \{0\} \to \mathbb{N}$, $r \mapsto \nu(r)$.
Hinweis: Machen Sie für $a, b \in R \setminus \{0\}$ eine Fallunterscheidung danach, ob $\varphi(a) \geq \varphi(b)$ gilt oder nicht und betrachten Sie für einen der Fälle mal $ab^{-1} \in F$. Vielleicht gilt dann ja sogar $ab^{-1} \in R$.
Bemerkung: Für jeden Körper $K$ erfüllt $K[[T]]$ diese Bedingung und ist somit euklidisch.

**Aufgabe 28**
Skizzieren Sie die Inklusionen zwischen den Klassen der Ringe, der integren Ringe, der faktoriellen Ringe, der Hauptidealringe, der euklidischen Ringe

und der Körper und geben Sie jeweils (ohne Beweis) Beispiele und Gegenbeispiele an.
Hinweis: Ein Beispiel für einen Hauptidealring, welcher nicht euklidisch ist, ist $R = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$.

## Irreduzibilität

**Aufgabe 29**
Sei $K$ ein Körper und $f \in K[T]$ ein lineares Polynom. Zeigen Sie, dass $f \in K[T]$ irreduzibel ist.

**Aufgabe 30**
Sei $R$ ein Ring, $r \in R$ ein irreduzibles Element und $u \in R^\times$. Zeigen Sie, dass dann auch $ur \in R$ irreduzibel ist.

**Aufgabe 31**
Sei $K$ ein Körper und $f \in K[T]$ ein Polynom vom Grad $d \geq 2$. Zeigen Sie, dass falls $f$ eine Nullstelle in $K$ hat, $f \in K[T]$ reduzibel sein muss.

**Aufgabe 32**
Sei $K$ ein Körper und und $f \in K[T]$.

(i) Zeigen Sie das sogenannte Wurzelkriterium (für Irreduzibilität):
Gilt $\deg(f) = 2$ oder $\deg(f) = 3$, so ist $f \in K[T]$ irreduzibel genau dann, wenn $f$ keine Nullstellen in $K$ besitzt.

(ii) Zeigen Sie, dass das Wurzelkriterium für Polynome höheren Grades nicht gilt.

**Aufgabe 33**
Fertigen Sie eine Liste aller Polynome $f \in \mathbb{F}_2[T]$ vom Grad $\deg(f) = 2$ an und testen Sie diese dann auf Irreduzibilität.

**Aufgabe 34**
Welche der folgenden Polynome $f \in K[T]$ sind irreduzibel?

(i) $f = 4T^5 + 93T^3 + 57T^2 + 6$, $K = \mathbb{Q}$

(ii) $f = T^2 - 6T + 1$, $K = \mathbb{F}_7$

(iii) $f = T^4 + 2T^2 + 1$, $K = \mathbb{Q}$

(iv) $f = 7T^7 + 49$, $K = \mathbb{Q}$

(v) $f = T^3 - T + 1$, $K = \mathbb{R}$

Hinweis: Bei (v) brauchen Sie ein analytisches Argument.

**Aufgabe 35**
Bestimmen Sie mit dem Fundamentalsatz der Algebra alle maximalen Ideale $\mathfrak{m} \subset \mathbb{C}[T]$.
Erinnerung: Der Fundamentalsatz der Algebra (in einer seiner Versionen) besagt, dass jedes nicht-konstante Polynom $f \in \mathbb{C}[T]$ in Linearfaktoren (mal Konstante) zerfällt.

# Körpertheorie

## Elementare Körpererweiterungen und die Gradformel

**Aufgabe 1**
Konstruieren Sie Körpererweiterungen $\mathbb{Q} \subset L_1$, $\mathbb{Q} \subset L_2$ und $\mathbb{F}_7 \subset E$ mit $[L_1 : \mathbb{Q}] = 3$, $[L_2 : \mathbb{Q}] = 4$ und $[E : \mathbb{F}_7] = 3$. Wie viele Elemente besitzt $E$? Ist $E$ aufgefasst als Ring isomorph zu $\mathbb{Z}/n\mathbb{Z}$ für ein $n \geq 2$?

**Aufgabe 2** Sei $n \in \mathbb{N}$ mit $n \geq 1$. Konstruieren Sie eine Körpererweiterung $\mathbb{Q} \subset L$ mit $[L : \mathbb{Q}] = n$.

**Aufgabe 3**
Sei $p > 0$ eine Primzahl. Zeigen Sie mit Hilfe folgender Anleitung, dass $K = \mathbb{F}_p$ stets eine Körpererweiterung $K \subset L$ vom Grad $[L : K] = 2$ besitzt:

(i) Betrachten Sie zunächst den Fall $p = 2$ und verwenden Sie z.B. eine geeignete Aufgabe aus dem Kapitel über Ringe.

(ii) Sei von nun an $p \geq 3$ beliebig. Zeigen Sie, dass die Menge

$$M = \{a \in \mathbb{F}_p \mid \text{a ist kein Quadrat}\} = \{a \in \mathbb{F}_p \mid \nexists b \in \mathbb{F}_p : b^2 = a\}$$

nicht leer ist, indem Sie den Gruppenhomomorphismus $\varphi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $a \mapsto a^2$ betrachten. Wie viele Elemente sind Quadrate und wie viele sind keine?

(iii) Konstruieren Sie die gewünschte Körpererweiterung $K \subset L$, indem Sie ausnutzen, dass $M$ nicht leer ist.

**Aufgabe 4**
In der vorherigen Aufgabe haben Sie unter anderem einen Körper $K$ mit $\operatorname{card}(K) = 4$ konstruiert. Geben Sie für diesen Körper die Verknüpfungstafeln der additiven und multiplikativen Gruppe an.

**Aufgabe 5**
Sei $K \subset L$ eine endliche Körpererweiterung, sodass $[L : K] = p > 0$ eine Primzahl ist. Zeigen Sie, dass $L = K(a)$ für jedes $a \in L \setminus K$ gilt.

**Aufgabe 6**
Sei $K \subset L$ eine Körpererweiterung und seien $K \subset E_1, E_2 \subset L$ zwei Zwischenkörper vom endlichen Grad $[E_i : K] = d_i$ mit $\operatorname{ggT}(d_1, d_2) = 1$. Zeigen Sie, dass $E_1 \cap E_2 = K$ gilt.

**Aufgabe 7**
Zeigen Sie, dass $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5} + \sqrt{7})$ gilt.

## Algebraische Körpererweiterungen

**Aufgabe 8**
Bestimmen Sie die Minimalpolynome der folgende Elemente $a \in \mathbb{C}$ über $K$:

(i) $a = \sqrt{2} + 1$, $K = \mathbb{Q}$

(ii) $a = 1 + i$, $K = \mathbb{Q}$

(iii) $a = \sqrt[3]{2}$, $K = \mathbb{Q}$

(iv) $a = \zeta_3$, $K = \mathbb{Q}$

(v) $a = \zeta_5 \sqrt[5]{3}$, $K = \mathbb{Q}$

(vi) $a = \zeta_5 \sqrt[5]{3}$, $K = \mathbb{Q}(\zeta_5 \sqrt[5]{3})$

**Aufgabe 9**
Welche der folgenden Aussagen gelten für alle Körpererweiterungen $K \subset L$ und alle Elemente $a \in L$?

(i) Es gilt $\deg(a) = 1$ genau dann, wenn $a \in K$.

(ii) Das Element $a$ ist algebraisch über $K$ genau dann, wenn $a^n$ algebraisch über K ist für ein $n \geq 2$.

(iii) Ist $a' \in L$ ein weiteres Element, sodass $a$ und $a'$ dasselbe Minimalpolynom haben, so gilt $K(a) \cong K(a')$.

(iv) Ist $a' \in L$ ein weiteres Element, sodass $K(a) \cong K(a')$, so haben $a$ und $a'$ dasselbe Minimalpolynom.

(v) Ist $a$ algebraisch über $K$, so zerfällt $\mu_a$ über $K(a)$ in Linearfaktoren.

(vi) Ist $a$ algebraisch über $K$, so ist $\mu_a$ über $K(a)$ reduzibel.

**Aufgabe 10**
Zeigen Sie, dass $\mathbb{Q} \subset \mathbb{R}$ eine unendliche Körpererweiterung ist.
Hinweis: Verwenden Sie ihr Wissen über Kardinalitäten oder konstruieren Sie einen geeigneten Zwischenkörper $\mathbb{Q} \subset E \subset \mathbb{R}$.

**Aufgabe 11**
Sei $K \subset L$ eine endliche Körpererweiterung. Zeigen Sie, dass $K \subset L$ algebraisch ist.

**Aufgabe 12** Sei $K$ ein beliebiger Körper. Geben Sie eine Körpererweiterung $K \subset L$ und ein transzendentes Element $a \in L$ an.

**Aufgabe 13**
Sei $K$ ein Körper und $a$ transzendent über $K$. Zeigen Sie mit Hilfe folgender Anleitung, dass $K \subset K(a)$ unendlich viele Zwischenkörper besitzt:

(i) Überlegen Sie sich zunächst, dass $a^2$ transzendent über $K$ ist.

(ii) Zeigen Sie nun, dass $K(a^2) \subsetneq K(a)$ eine echte Inklusion ist.

(iii) Nutzen Sie die vorherige Teilaufgabe um unendlich viele Zwischenkörper zu konstruieren.

**Aufgabe 14**
Sei $K \subset L$ eine algebraische Körpererweiterung. Seien außerdem $a, b \in L$ mit Graden $\deg(a) = m$, $\deg(b) = n$, sodass $\mathrm{ggT}(m, n) = 1$. Zeigen Sie, dass $E = K(a, b)$ den Grad $[E : K] = m \cdot n$ hat.

## Normale Körpererweiterungen/Zerfällungskörper

**Aufgabe 15**
Sei $K \subset L$ algebraisch und seien $K \subset E_i \subset L$, $i \in I$, eine Familie von Zwischenkörpern, sodass $K \subset E_i$ für alle $i \in I$ normal ist. Zeigen Sie, dass dann auch $K \subset E$ normal ist, wobei $E$ der Durchschnitt über die $E_i$, $i \in I$, ist.

**Aufgabe 16**
Sei $K \subset L$ der Zerfällungskörper eines Polynomes $f \in K[T]$. Beschreiben Sie, warum $[L : K] \leq \deg(f)!$ gilt.

**Aufgabe 17**
Sei $K$ ein Körper. Zeigen Sie, dass jede endliche Körpererweiterung $K \subset E$ als Zwischenkörper einer endlichen normalen Körpererweiterung auftritt.

**Aufgabe 18**
Sei $K \subset L$ eine Körpererweiterung vom Grad $[L : K] = 2$. Zeigen Sie, dass $K \subset L$ normal ist.

**Aufgabe 19**
Zeigen Sie mit Hilfe folgender Anleitung, dass Normalität von Körpererweiterungen nicht transitiv ist, also Körper $K \subset E \subset L$ existieren, sodass $K \subset E$ und $E \subset L$ normal sind, aber $K \subset L$ nicht normal ist:

(i) Betrachten Sie die Körpererweiterung $K = \mathbb{Q} \subset \mathbb{R}$ und $a = \sqrt[4]{2} \in \mathbb{R}$. Zeigen Sie, dass $[L : K] = 4$ gilt, wobei $L = \mathbb{Q}(a)$.

(ii) Konstruieren Sie einen Zwischenkörper $K \subset E \subset L$, sodass $K \subset E$ und $E \subset L$ normal sind.
Hinweis: Um Letzteres sicherzustellen, könnte die vorherige Aufgabe nützlich sein.

(iii) Zeigen Sie, dass $K \subset L$ nicht normal ist.

**Aufgabe 20**
Bestimmen Sie den Zerfällungskörper $\mathbb{Q} \subset L$ folgender Polynome $f \in \mathbb{Q}[T]$ und den Grad der Körpererweiterung $[L : \mathbb{Q}]$:

(i) $f = T^2 + 4$

(ii) $f = T^4 - 2$

(iii) $f = T^4 - 12T^2 + 35$

**Aufgabe 21**
Konstruieren Sie Körper $K \subset E \subset L$, sodass $K \subset L$ normal ist, aber $K \subset E$ nicht normal ist.

## Separable Körpererweiterungen

**Aufgabe 22**
Welche der folgenden Polynome $f \in K[T]$ sind separabel?

(i) $f = T^3 + 1$, $K = \mathbb{Q}$

(ii) $f = T^3 + T^2 + 6T + 6$, $K = \mathbb{F}_7$

(iii) $f = T^3 - T + 1$, $K = \mathbb{R}$

**Aufgabe 23**
Sei $K$ ein Körper und $f = aT^2 + bT + c \in K[T]$ ein quadratisches Polynom, also $a \neq 0$. Dann ist die Diskriminante von $f$ gegeben durch $\Delta = b^2 - 4ac$. Drücken Sie $\Delta$ durch $a$ und durch die beiden Nullstellen $\omega_1, \omega_2 \in K^{\mathrm{alg}}$ von $f$ aus und folgern Sie, dass f separabel ist genau dann, wenn $\Delta \neq 0$ gilt.

**Aufgabe 24**
Sei $p > 0$ eine Primzahl und $K$ ein Körper der Charakteristik p. Zeigen Sie, dass $(a+b)^p = a^p + b^p$ für alle $a, b \in K$ gilt und konstruieren Sie ein irreduzibles, aber nicht separables Polynom $f \in F[T]$ für einen konkreten Körper $F$ der Charakteristik $p$.
Hinweis: Betrachten Sie $F = K(T)$.

**Aufgabe 25**
Sei $p > 0$ eine Primzahl und $K$ ein Körper der Charakteristik p. Zeigen Sie mit Hilfe folgender Anleitung, dass das polynom $f(T) = T^p - T - \lambda \in K[T]$ separabel ist:

(i) Zeigen Sie mit dem Satz von Lagrange, dass $a^p = a$ für alle $a \in \mathbb{F}_p$ gilt.

(ii) Folgern Sie, dass $f(T) = f(T+a)$ für alle $a \in \mathbb{F}_p$ gilt.

(iii) Wählen Sie eine Nullstelle $\omega \in K^{\text{alg}}$ von $f$, geben Sie alle anderen Nullstellen in Abhängikeit von $\omega$ an und beenden Sie den Beweis.

**Aufgabe 26**
Sei $K$ ein Körper.

(i) Zeigen Sie, dass ein irreduzibles Polynom $f \in K[T]$ separabel ist genau dann, wenn $f' \neq 0$ gilt.

(ii) Folgern Sie, dass jedes irreduzible Polynom über einem Körper der Charakteristik 0 separabel ist.

Hinweis: Nehmen Sie bei (i) ohne Einschränkung an, dass $f$ normiert ist.

**Aufgabe 27**
Sei $p > 0$ eine Primzahl, $K$ ein Körper der Charakteristik $p$ und $f \in K[T]$ ein irreduzibles Polynom. Verwenden Sie den ersten Aufgabenteil der vorherigen Aufgabe um zu zeigen, dass die folgenden beiden Aussagen äquivalent sind:

(i) Das Polynom $f$ ist nicht separabel.

(ii) Es gilt $f \in K[T^p]$.

**Aufgabe 28**
Geben Sie einen Körper $K$ sowie zwei Körpererweiterungen $K \subset L, L'$ an, sodass $K \subset L$ separabel ist und $K \subset L'$ nicht separabel ist.

## Galois-Erweiterungen

### Aufgabe 29

(i) Zeigen Sie, dass $\mathbb{R} \subset \mathbb{C}$ galoisch ist.

(ii) Bestimmen Sie die Galois-Gruppe $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Ist sie isomorph zu einer Ihnen bekannten Gruppe?

(iii) Gibt es eine Körpererweiterung $\mathbb{C} \subset L$ mit $[L : \mathbb{C}] \geq 2$?.

### Aufgabe 30

Sei $K \subset L$ eine Galois-Erweiterung mit Galois-Gruppe $\mathrm{Gal}(L/K) \cong \mathbb{Z}/18\mathbb{Z}$. Bestimmen Sie die Anzahl der Zwischenkörper $K \subset E \subset L$ und geben Sie für alle Zwischenkörper $K \subset E, E' \subset L$ mit $E \subset E'$ die Grade $[E' : E]$ an.

### Aufgabe 31

Sei $p > 0$ eine Primzahl und $K \subset L$ eine Galois-Erweiterung vom Grad $[L : K] = p^2$. Zeigen Sie, dass es einen Zwischenkörper $K \subset E \subset L$ mit $[E : K] = p$ gibt, sodass $K \subset E$ normal ist.
Hinweis: Was wissen Sie über Gruppen der Ordnung $p^2$?

### Aufgabe 32

Sei $K \subset L$ eine Galois-Erweiterung vom Grad $[L : K] = n \geq 2$. Zeigen Sie, dass es für alle $1 \leq j \leq r$ einen Zwischenkörper $K \subset E_j \subset L$ mit

$$[E_j : K] = \prod_{\substack{i=1 \\ i \neq j}}^{r} p_i^{\nu_i}$$

gibt, wobei $n = \prod_{i=1}^{r} p_i^{\nu_i}$ die Primfaktorzerlegung von $n$ ist.
Hinweis: Verwenden Sie einen der Sylow-Sätze.

### Aufgabe 33

Sei $p > 0$ eine Primzahl und $f \in \mathbb{Q}[T]$ ein irreduzibles Polynom vom Grad $\deg(f) = p$. Nach dem Fundamentalsatz der Algebra besitzt $f$ über $\mathbb{C}$ also $p$ verschiedene Nullstellen $a_1, ..., a_p$. Angenommen, genau zwei dieser Nullstellen liegen in $\mathbb{C} \setminus \mathbb{R}$. Zeigen Sie mit Hilfe folgender Anleitung, dass dann $G = \mathrm{Gal}(L/\mathbb{Q}) = S_p$ gilt, wobei $\mathbb{Q} \subset L$ der Zerfällungskörper von $f$ ist:

(i) Zeigen Sie zunächst, dass $p$ die Ordnung von $G$ teilt, indem Sie die Gradformel auf einen geeigneten Zwischenkörper anwenden. Folgern Sie dann, dass $G$ einen $p$-Zykel enthält.

(ii) Zeigen Sie, dass $G$ eine Transposition enthält.

(iii) Zitieren Sie eine geeignete Aufgabe aus dem Kapitel über Gruppen oder überlegen Sei sich, warum nun bereits $G = S_p$ gilt.

Hinweis: Betrachten Sie für (ii) die beiden Nullstellen, welche in $\mathbb{C} \setminus \mathbb{R}$ liegen.

**Aufgabe 34**
Sei $K \subset L$ eine Körpererweiterung, wobei $K$ der Primkörper von $L$ ist und seien $a_1, ..., a_n \in L$ algebraisch über $K$. Zeigen Sie mit Hilfe folgender Anleitung, dass Elemente $\sigma \in \mathrm{Aut}(K(a_1, ..., a_n)/K)$ durch die Bilder der $a_1, ..., a_n$ bereits festgelegt werden:

(i) Seien $E$ und $E'$ Körper und $f, g : E \to E'$ zwei Körperhomomorphismen. Zeigen Sie, dass die Menge $\mathrm{Eq}(f, g) = \{a \in E \mid f(a) = g(a)\}$ ein Körper ist.

(ii) Folgern Sie, dass $\mathrm{Aut}(K) = \{id_K\}$ für jeden Primkörper $K$ gilt. Wir erhalten also $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}_\mathbb{Q}\}$ und $\mathrm{Aut}(\mathbb{F}_p) = \{\mathrm{id}_{\mathbb{F}_p}\}$ für jede Primzahl $p > 0$.

(iii) Nutzen Sie die Form eines $a \in K(a_1, ..., a_n)$ aus und beenden Sie den Beweis.

**Aufgabe 35**
Bestimmen Sie die folgenden beiden Galois-Gruppen:

(i) $\mathrm{Gal}(L/\mathbb{Q})$, wobei $\mathbb{Q} \subset L$ der Zerfällungskörper von $T^3 - 2 \in \mathbb{Q}[T]$ ist

(ii) $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$

Bemerkung: Sie sollten auch begründen, warum obige Körpererweiterungen überhaupt galoisch sind.