1. Symmetrische Gruppen

1. Bestimme alle Untergruppen der symmetrischen Gruppe S_4. Zeichne den entsprechenden Untergruppen-Verband.

2. (a) Die Gruppe S_n wird von den Elementen $(1,2), (2,3), \ldots, (n-1,n)$ erzeugt.

(b) Die Gruppe S_n wird von den Elementen $(1,2)$ und $(2,3,\ldots n)$ erzeugt.

3. (a) Die Partition der Zykellängen von $\sigma \in S_n$ sei $(\lambda_1, \ldots, \lambda_t)$. Man zeige: Genau dann gehört σ zur A_n, wenn $t \equiv n \mod 2$ gilt.

(b) Bestimme die Ordnungen der Elemente der Gruppe A_{20}.

4. (a) Man beschreibe alle Elemente von Primzahlordnung in der S_n. Wieviele Elemente der Ordnung 3 gibt es in der S_{10} ?

(b) Sei σ ein n-Zykel in der S_n. Man bestimme alle Elemente $\tau \in S_n$ mit $\sigma \cdot \tau = \tau \cdot \sigma$.

Übungszettel mit meist 4 Übungsaufgaben werden in der Donnerstagsvorlesung verteilt. Es sollten immer alle Aufgaben bearbeitet werden. Die Aufgaben sind selbständig zu lösen. Bitte schreiben Sie Ihre Lösungen kurz und prägnant, aber mit vollständigen Zwischentexten, leserlich auf DIN A4-Blätter. Die Aufgaben können in Zweiergruppen bearbeitet und abgegeben werden. Pro Zweiergruppe soll für jede Aufgabe nur eine Lösung abgegeben werden, dabei muß beim Aufschreiben der Lösungen abgewechselt werden. Sofern auf dem Lösungszettel nichts anderes vermerkt ist, wird davon ausgegangen, daß jeder der Beteiligten mit **jeder** der notierten Lösungen vertraut ist und bereit ist, diese vorzuführen.

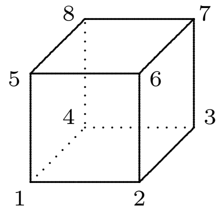
Abgabe spätestens am folgenden Donnerstag, 10:10 Uhr ins Postfach des Übungsleiters (Karsten Schmidt). Die Lösungen werden in den Übungsstunden der darauffolgenden Woche besprochen.

Für jede vollständig gelöste Aufgabe gibt es 4 Punkte. Für einen Übungsschein (zur Bescheinigung der erfolgreichen Teilnahme) sind 50% der Punkte erforderlich. Wer zuwenige Punkte haben sollte, kann eine mündliche Prüfung über den Stoff der Vorlesung und der Übungen ablegen.

Routine-Übungen.

A. Symmetrische Gruppen

1. Betrachte folgenden Würfel



Wie lautet die Zykelbeschreibung folgender Permutationen der Eckenmenge $\{1, 2, \ldots, 8\}$?

a) Spiegelung an der zu $\overline{14}$ senkrechten Ebene.

b) Spiegelung an der Ebene, die durch die Ecken $1, 2, 3, 4$ geht.

c) Drehung um $120°$ um die Achse durch 1 und 7.

d) Drehung um $180°$, die Drehachse gehe durch den Mittelpunkt der Strecke $\overline{5}6$.

e) Drehung um $90°$, die Drehachse gehe durch den Mittelpunkt des Quadrats mit den Ecken $1, 2, 5, 6$.

2. (a) Berechne alle Potenzen der Permutation

$$(12345)(67)$$

(insgesamt sollte man 10 Elemente erhalten. Warum?)

(b) Sei σ eine Permutation mit Partition $(\lambda_1, \ldots, \lambda_m)$. Dann ist die Ordnung von σ gerade das k.g.V. der Zahlen $\lambda_1, \ldots, \lambda_t$.

3. Man berechne eine Zykelbeschreibung von

$$(1, 2, 3) \circ (1, 7, 6, 5) \circ (1, 3, 5, 7) \circ (1, 2) \circ (1, 7)$$

(in der S_8).

B. Beispiele von Gruppen und Untergruppen

(1) Bestimme alle Untergruppen von $(\mathbb{Z}, +)$.

(2) Betrachte die Symmetriegruppe eines regelmäßigen n-Ecks. Ist n eine Primzahl, so geben man alle Untergruppen an.

(3) Sei $n \in \mathbb{N}_1$. Die komplexen Zahlen der Form $e^{\frac{2\pi i a}{n}}$, mit $a \in \mathbb{Z}$ heißen (n-te) Einheitswurzeln.

Sei E_n die Menge der n-ten Einheitswurzeln. Zeige

(a) Die Menge E_n ist bezüglich der Multiplikation komplexer Zahlen eine zyklische Gruppe der Ordnung n.

(b) Es gilt genau dann $E_n \subseteq E_m$, wenn n ein Teiler von m ist.

(c) Bestimme alle Untergruppen von

$$E_5, \quad E_{25}, \quad E_{125}, \quad E_{1000}, \quad E_{30}.$$

Zeichne die entsprechenden Untergruppen-Verbände.

C. Grundsätzliches

(1) Seien U, V Untergruppen einer Gruppe. Zeige: $U \cap V$ ist eine Untergruppe von G.

(2) Sei eine Familie U_i von Untergruppen von G (mit $i \in I$) gegeben. Zeige: $\bigcap_{i\in I} U_i$ ist eine Untergruppe von G.

(3) Folgerung: Ist S eine Teilmenge einer Gruppen, so gibt es eine eindeutig bestimmte kleinste Untergruppe von G, die S enthält, nämlich den Durchschnitt aller Untergruppen von G, die S enthalten. (Man nennt diese Untergruppe die von S erzeugte Untergruppe.)

D. Konstruktion: Direktes Produkt

Seien G, H Gruppen. Sei $G \times H$ die Menge der Paare (g, h) mit $g \in G, h \in H$, mit folgender Multiplikation:

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2).$$

(1) Zeige: $G \times H$ ist wieder eine Gruppe.

(2) Bestimme alle Untergruppen von

$$C_2 \times C_3, \quad C_2 \times C_5, \quad C_3 \times C_7,$$
$$C_2 \times C_2, \quad C_3 \times C_3,$$
$$C_2 \times C_2 \times C_2.$$

Zeige dabei: Die ersten drei Gruppen sind zyklisch, die übrigen nicht.

E. Beweise

(1) Zeige: Hat jedes Element einer Gruppe Ordnung 1 oder 2, so ist die Gruppe kommutativ.

(2) Ist N ein Normalteiler einer Gruppe und gilt $|N| = 2$, so liegt N im Zentrum.

(3) Ist U eine Untergruppe einer Gruppe G und gilt $G : H = 2$, so ist U ein Normalteiler.

2. Untergruppen, Nebenklassen. Diesmal 5 Aufgaben.

5. Noch einmal die Aufgabe 1: Bestimme alle Untergruppen des symmetrischen Gruppe S_4. Diesmal mit Anleitung (siehe Rückseite); es sollen also der Anleitung folgend die Details des Beweises notiert werden.

6. Sei ϕ: $G \to H$ ein Gruppen-Homomorphismus mit Kern N und Bild B. Sei U eine Untergruppe von G, sei V eine Untergruppe von H. Zeige:

$$\phi^{-1}\phi(U) = UN \quad \text{und} \quad \phi\phi^{-1}(V) = V \cap B.$$

Folgere daraus, daß ϕ eine Bijektion zwischen einerseits den Untergruppen von G, die N enthalten, und andererseits den Untergruppen von B liefert.

7. Sei G eine Gruppe.

(a) Seien $U \subseteq V \subseteq G$ Untergruppen von G mit endlichem Index. Zeige:

$$[G : U] = [G : V] \cdot [V : U].$$

(b) Seien U_1, U_2 Untergruppen von G mit endlichem Index. Man zeige, daß auch $U_1 \cap U_2$ endlichen Index hat, und daß gilt

$$[G : U_1 \cap U_2] \leq [G : U_1] \cdot [G : U_2].$$

Anleitung: Sei $\mathcal{U}_i$ die Menge der Linksnebenklassen von G nach U_i und $\mathcal{U}$ die Menge der Linksnebenklassen von G nach $U_1 \cap U_2$. Zeige: Durch $g(U_1 \cap U_2) \mapsto (gU_1, gU_2)$ erhält man eine injektive Abbildung $\mathcal{U} \to \mathcal{U}_1 \times \mathcal{U}_2$ (zu zeigen ist vor allem auch, daß diese Zuordnung wohldefiniert ist).

(c) Folgere aus (a) und (b) daß gilt: Sing U_1, U_2 Untergruppen von G mit endlichem Index und sind die Indizes $[G : U_1]$ und $[G : U_2]$ teilerfremd, so gilt

$$[G : U_1 \cap U_2] = [G : U_1] \cdot [G : U_2].$$

8. Sei U eine Untergruppe von G mit Index n. Zeige: *Es gibt einen Normalteiler N in G mit endlichem Index, der in U enthalten ist.*

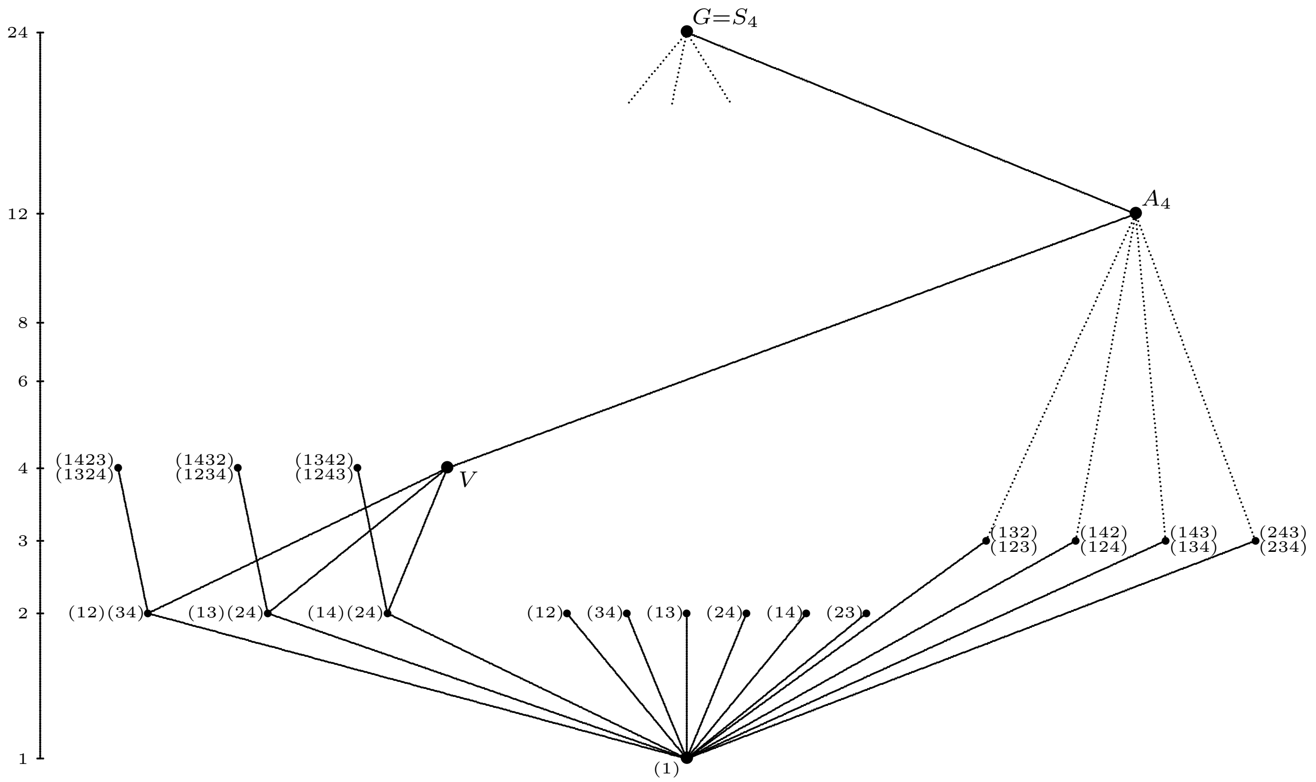
Anleitung: Sei $\mathcal{U}$ die Menge der Linksnebenklassen von U in G. Nach Voraussetzung ist dies eine Menge der Kardinalität n und die Linksmultiplikation mit einem Element $g \in G$ permutiert diese Linksnebenklassen, liefert also eine Permutation in $S_{\mathcal{U}} = S_n$. Auf diese Weise erhalten wir einen Gruppen-Homomorphismus $G \to S_n$, dessen Kern in U enthalten ist ....

9. (a) Seien U, V Untergruppen der Gruppe G. Zeige: Genau dann ist $UV = \{uv \mid u \in U, v \in V\}$ eine Untergruppe von G, wenn $UV = VU$ gilt.

(b) Man gebe Beispiele von Untergruppen U, V einer Gruppe G an, für die UV keine Untergruppe ist.

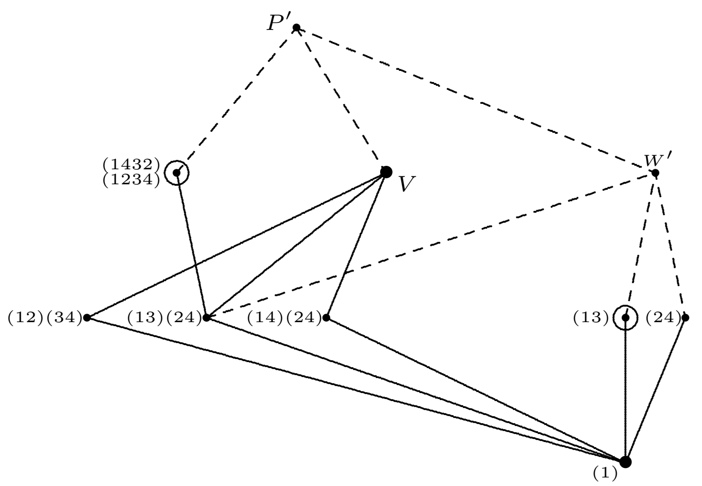
Anleitung zur Konstruktion des Untergruppen-Verbands der S_4.

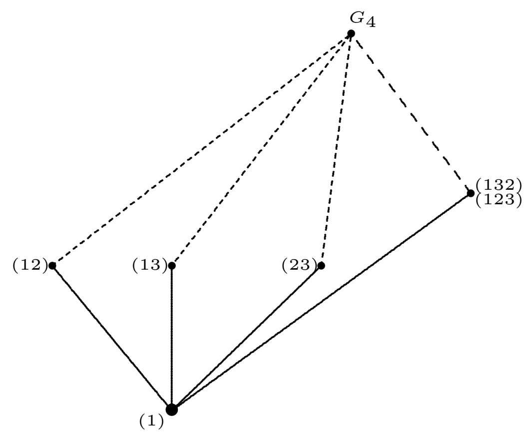
1. Als bekannt werde vorausgesetzt: der Untergruppenverband der A_4 und alle zyklischen Untergruppen der S_4, also das folgende Bild:



2. (a) Betrachte das Erzeugnis von (1234) und (13), dies liefert eine **Diedergruppe** D_4, hier bezeichnet als P'. (Analog erhält man zwei weitere Diedergruppen P und P''.)

(b) Bezeichne mit G_4 den Stabilisator von 4 in G, also die Untergruppe aller $g \in G$ mit $g(4) = 4$. Diese Untergruppe G_4 ist gerade die Permutationsgruppe auf der Menge $\{1, 2, 3\}$, also eine S_3. (Analog erhält man drei weitere Untergruppen G_1, G_2, G_3.)





Damit hat man schon **alle** Untergruppen konstruiert (aber das ist erst noch zu zeigen)!

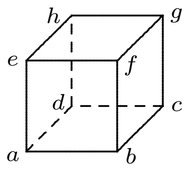
3. Sei also U eine Untergruppe von G. Wir können annehmen: $U \not\subseteq A_4$.

Fall 1: Es enthalte U einen 4-Zykel, obdA: $(1234) \in U$. Zeige: Entweder gilt $U \subseteq P'$ oder aber $U = G$.

Fall 2: Es enthalte U keinen 4-Zykel. Dann enthält U eine Transposition, etwa $(12) \in U$. Zeige: Endweder $U \subseteq G_3$ oder $U \subseteq G_4$ oder $U = G$.

3. Untergruppen. Wieder 5 Aufgaben.

10. Noch einmal Aufgabe 1. Wie wir wissen ist die Drehgruppe des Würfels isomorph zu S_4. Man suche nach Beschriftungen des Untergruppenverbands der S_4, die sich nur auf den Würfel beziehen. Zu ändern sind also die dort notierten Bezeichungen der Elemente und der Untergruppen. Zur Standartisierung bezeichnen wir die Ecken des Würfels wie folgt:



und nummerieren die Raumdiagonalen (oder Eckenpaare) auf folgende Weise:

$$1 = \{a, g\}, \quad 2 = \{b, h\}, \quad 3 = \{c, e\}, \quad 4 = \{d, f\}.$$

Zu untersuchen ist also: Welche Sorte von Drehung entspricht welchem Zykeltyp? Und: Wie lassen sich die 30 Untergruppen geometrisch interpretieren?

11. Sei p eine Primzahl. Sei k ein Körper mit p Elementen. Zeige:

(a) Die Menge P der unipotenten oberen Dreiecksmatrizen ist eine p-Untergruppe von $G = \mathrm{GL}(n, k)$ und p ist kein Teiler von $[G : P]$.

(b) Ebenso ist die Menge P' der unipotenten unteren Dreiecksmatrizen eine p-Untergruppe.

(c) Man gebe ein Element $g \in \mathrm{GL}(n, k)$ mit $gPg^{-1} = P'$ an.

12. Sei p eine Primzahl, sei $p \le n \le 2p - 1$.

(a) Zeige: p teilt $n!$, aber p^2 teilt nicht $n!$.

(b) Bestimme die Anzahl a der Untergruppen der Ordnung p.

Zeige, daß gilt a ist ein Teiler von $n!$ und $a \equiv 1 \mod p$.

13. Sei X ein platonischer Körper (also ein Tetraeder, Würfel, Oktaeder, Dodekaeder oder Ikosaeder). Sei G_X die volle Symmetriegruppe (aller Drehungen und Spiegelungen) und H_X die Drehgruppe von X. Bestimme jeweils die Ordnung von G_X und H_X (wenn möglich auf verschiedene Weisen).

14. Sei $n \in \mathbb{N}_1$. Die komplexen Zahlen der Form $e^{\frac{2\pi i a}{n}}$, mit $a \in \mathbb{Z}$ heißen (n-te) Einheitswurzeln.

Sei E_n die Menge der n-ten Einheitswurzeln.

(a) Zeige, daß E_n bezüglich der Multiplikation komplexer Zahlen eine zyklische Gruppe der Ordnung n.

(b) Bestimme alle Untergruppen von E_5, $\quad E_{25}$, $\quad E_{125}$, $\quad E_{10\,000}$, $\quad E_{30}$, $\quad E_{1155}$.
Zeichne die entsprechenden Untergruppen-Verbände.

4. Gruppen-Operationen

15. Eine Gruppe G der Ordnung 55 operiere auf einer Menge mit 19 Elementen. Man zeige, daß es mindestens 3 Fixpunkte gibt.

16. Sei G eine p-Gruppe. Zeige: Ein Normalteiler N von G der Ordnung p liegt immer im Zentrum.

(Hinweis: G operiert auf N vermöge Konjugation. Betrachte die möglichen Bahnenlängen.)

17. Zeige: Eine Gruppe der Ordnung 123 456 ist nicht einfach.

18. Sei $|G| = pq$, mit Primzahlen $p < q$. Zeige:

(a) G hat genau eine q-Sylowgruppe.

(b) Hat G nicht nur eine p-Sylowgruppe, so ist $q = 1 + kp$ mit $k > 0$.

Zusatz: Es folgt also, daß die Ordnung einer einfachen nicht-abelschen Gruppe weder eine Primzahlpotenz noch von der Form pq mit Primzahlen p, q sein kann. Welche Zahlen $1 \leq n \leq 59$ sind weder Primzahlpotenzen noch von der Form pq mit Primzahlen p, q?

19. Zeige: Es gibt genau zwei Isomorphieklassen von Gruppen der Ordnung p^2, nämlich die der Gruppe C_{p^2} und die der Gruppe $C_p \times C_p$.

Übungsscheine (= Leistungsnachweise).
Für den Erhalt eines Scheins sind mindestens 50 % der erreichbaren Punkte erforderlich. Dabei wird erwartet, daß auch nach Erreichen dieser Punktzahl weiterhin Lösungen der Übungsaufgaben abgegeben werden und in den Übungsgruppen mitgearbeitet wird. Für Lehramtsstudenten gibt es auf Wunsch auch sogenannte **qualifizierte Studiennachweise,** dafür sind (neben der aktiven Teilnahme an den Übungsgruppen) mindestens 35 % der erreichbaren Punkte erforderlich.

Noch einmal: **19.** Zeige: Es gibt genau zwei Isomorphieklassen von Gruppen der Ordnung p^2, nämlich die der Gruppe C_{p^2} und die der Gruppe $C_p \times C_p$.

Es darf folgendes Lemma verwendet werden: Sind U, V zwei Normalteiler einer Gruppe G mit $UV = G$ und $U \cap V = \{1\}$, so ist G isomorph zu $U \times V$ (siehe Leitfaden, p.17).

5. Körper

20. Sei K ein Körper. Zeige: K besitzt einen kleinsten Unterkörper K_0. Ist $n \cdot 1_K \neq 0$ für alle natürlichen Zahlen $n \geq 1$, so ist K_0 zu $\mathbb{Q}$ isomorph. Gibt es eine natürliche Zahl $n \geq 1$ mit $n \cdot 1_K = 0$, so ist die kleinste derartige Zahl eine Primzahl p, und K_0 hat genau p Elemente, nämlich die Elemente $t \cdot 1_K$ mit $0 \leq t < p$.

21. Bestimme den kleinsten Unterkörper K von $\mathbb{R}$, der die beiden Zahlen $\sqrt{2}$, $\sqrt{3}$ enthält. Bestimme die Dimension von K als $\mathbb{Q}$-Vektorraum.

Hinweis: K enthält natürlich $\mathbb{Q}$, und auch alle $\mathbb{Q}$-Vielfache von $\sqrt{2}$ und von $\sqrt{3}$, also alle Linearkombinationen $c_0 + c_1\sqrt{2} + c_3\sqrt{3}$ mit $c_0, c_1, c_2 \in \mathbb{Q}$. Ist die Menge dieser Elemente unter Multiplikation abgeschlossen? Nein, also muß man weitere Elemente betrachten .... Sobald man eine elementweise Beschreibung von K gefunden hat, geht es darum, eine Basis zu bestimmen: insbesondere ist zu zeigen, daß gewisse Elemente (wie 1, $\sqrt{2}$, $\sqrt{3}$, ...) linear unabhängig sind.

22. Bestimme die Minimalpolynome der folgenden komplexen Zahlen über $\mathbb{Q}$

$$\sqrt{2+\sqrt[3]{2}}, \qquad \sqrt{3}+\sqrt[5]{3}, \qquad \sqrt[3]{2}+i\sqrt[5]{2}.$$

23. Seien $p \neq q$ Primzahlen. Sei L der kleinste Unterkörper von $\mathbb{R}$, der die Zahlen $\sqrt{p}$ und $\sqrt[3]{q}$ enthält. Zeige: L wird vom Element $\sqrt{p} \cdot \sqrt[3]{q}$ erzeugt und hat Grad 6 über $\mathbb{Q}$.

6. Kreisteilungspolynome und Körpererweiterungen

Betrachte die folgende n-te Einheitswurzel $\zeta_n = e^{\frac{2\pi i}{n}}$ in $\mathbb{C}$ und ihre Potenten ${\zeta_n}^t$ mit $1 \leq t \leq n$. Setze $\Phi_n(X) = \prod_{1\leq t\leq n,(t,n)=1}(X - {\zeta_n}^t)$, man nennt Φ_n das n-te Kreisteilungspolynom.

24. Zeige:

(a) $X^n - 1 = \prod_{1\leq t\leq n}(X - {\zeta_n}^t)$

(b) $X^n - 1 = \prod_{d|n} \Phi_d(X)$ (dabei soll das Produkt über alle natürlichen Zahlen d gebildet werden, die n teilen).

(c) Es ist $\Phi_n(X) \in \mathbb{Q}[X]$. (Verwende (b) und Induktion).

25. Zeige:

(a) Ist p eine Primzahl, so ist $\Phi_p = X^{p-1} + \cdots + X + 1$.

(b) Bestimme die Kreisteilungspolynome Φ_n für $1 \leq n \leq 30$.

26. Sei $K \subset L$ eine Körpererweiterung vom Grad 2. Zeige:

(a) Es braucht in L kein Element α mit $L = K(\alpha)$ und $\alpha^2 \in K$ zu geben. (Betrachte zum Beispiel: $K = \mathbb{F}_2$ und $L = K[X]/(X^2 + X + 1)$.)

(b) Ist die Charakteristik von K nicht 2, so gibt es ein Element $\alpha \in L$ mit $L = K(\alpha)$ und $\alpha^2 \in K$.

27. Bestimme in $K = \mathbb{Q}(\sqrt{2}, i)$ alle Elemente α mit $\alpha^2 \in \mathbb{Q}$. Wie sehen demnach die Unterkörper von K aus?

7. Körpererweiterungen

28. Zeige: Ist $\mathbb{Q} \subset L$ eine Körpererweiterung vom Grad 2, so ist $L = \mathbb{Q}[\alpha]$ mit $\alpha^2 = -1$ oder $\alpha^2 = p_1 \cdots p_t$ oder $\alpha^2 = -p_1 \cdots p_t$, und dabei sind $p_1, \dots p_t$ paarweiese verschiedenen Primzahlen und es ist $t \geq 1$.

29. Sei ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$ mit $n \geq 3$. Zeige

$$\big[\mathbb{Q}[\zeta] : \mathbb{Q}[\zeta + \zeta^{-1}]\big] = 2$$

auf folgende Weise:

(a) Es ist $\mathbb{Q}[\zeta + \zeta^{-1}]$ ein echter Unterkörper von $\mathbb{Q}[\zeta]$. Und

(b) ζ ist eine Nullstelle von $T^2 - (\zeta + \zeta^{-1})T + 1$.

30. Sei nun ζ eine primitive 5-te Einheitswurzel in $\mathbb{C}$. Zeige, daß $X^2 + X + 1$ das Minimalpolynom von $\zeta + \zeta^{-1}$ über $\mathbb{Q}$ ist. Bestimme auf diese Weise $[\mathbb{Q}[\zeta] : \mathbb{Q}]$.

31. Sei $K \subseteq L$ eine Körpererweiterung. Das Polynom $f \in K[X]$ zerfalle über L in Linearfaktoren, etwa

$$f = (T - \alpha_1) \cdots (T - \alpha_n).$$

(a) Zeige: $K[\alpha_1, \dots, \alpha_{n-1}]$ ist ein Zerfällungskörper von f.

(b) Man gebe ein Beispiel mit $n \geq 3$ an, daß $K[\alpha_1, \dots, \alpha_{n-2}]$ kein Zerfällungskörper von f ist.

32. Sei $K \subseteq K[\alpha]$ eine Körpererweiterung, das Minimalpolynom von α über K sei von der Form $f = T^n - a$ mit $a \in K$. Zeige: Genau dann zerfällt f in $K[\alpha]$ in Linearfaktoren, wenn K alle n-ten Einheitswurzeln enthält (d.h.: wenn $T^n - 1$ in K in Linearfaktoren zerfällt).

8. Polynome, Körpererweiterungen

33. Seien $a, b \in \mathbb{Q}$. Betrachte das Polynom $f = X^3 + aX + b \in \mathbb{Q}[X]$. Seien $\alpha_1, \alpha_2, \alpha_3$ die Wurzeln von f. Zeige, daß gilt

$$(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = -4a^3 - 27b^2.$$

(Hinweis: Wegen $f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$ läßt sich ein Koeffizientenvergleich durchführen.

34. Folgere aus dem Ergebnis der Aufgabe 33: Genau dann hat der Zerfällungskörper von f Grad 3 über $\mathbb{Q}$, wenn f irreduzibel und $-4a^3 - 27b^2$ ein Quadrat in $\mathbb{Q}$ ist.

35. Sei K ein Körper, $K[T]$ der Polynomring in einer Variablen. Für $f = \sum_{i=0}^n c_i T^i$ definiert man $f' = \sum_{i=1}^n i c_i T^{i-1}$ und nennt dies die *Ableitung* von f.

(a) Zeige: Sind $f, g \in K[T]$, so gilt $(fg)' = f'g + fg'$.

(b) Folgere daraus: Sind $f, g \in K[T]$ und ist g^t mit $t \in \mathbb{N}_1$ ein Teiler von f, so ist g^{t-1} ein Teiler von f'. Insbesondere gilt: Hat f eine doppelte Nullstelle α, so ist α Nullstelle von f'.

36. (a) Zeige: Jede Körpererweiterung von Grad 2 ist normal.

(b) Zeige: $\mathbb{Q} \subset \mathbb{Q}[\sqrt[4]{2}]$ ist nicht normal.

(c) Gibt es Körpererweiterungen $K_1 \subset K_2 \subset K_3$ mit $K_1 \subset K_2$ normal, $K_2 \subset K_3$ normal, aber $K_1 \subset K_3$ nicht normal?

37. Sei K ein Körper der Charakteristik p, dabei sei p eine Primzahl. Sei $a \in K$. Betrachte das Polynom $f = T^p - T - a$. Zeige:

(a) Ist α eine Nullstelle von f in einem Oberkörper von K, so ist auch $\alpha + 1$ eine Nullstelle.

(b) f ist separabel.

(c) Besitzt f keine Nullstelle in K, so ist f irreduzibel.

9.

38. Sei p eine Primzahl. (a) Sei K ein Körper der Charakteristik p. Sei $K \subseteq L$ eine Körpererweiterung mit $[L : K] = p^2$. Es gebe $u, v \in L$ mit $L = K[u, v]$ und $u^p, v^p \in K$. Zeige: Jedes Element $\alpha \in L \setminus K$ hat ein Minimalpolynom der Form $T^p - c$ mit $c \in K$. Insbesondere gibt es kein Element $w \in L$ mit $L = K[w]$.

(b) Sei k ein Körper der Charakteristik p, sei L der Quotientenkörper des Polynomrings $k[X, Y] = k[X][Y]$ in zwei Variablen mit Koeffizienten in k. Sei K der von X^p und Y^p erzeugte Zwischenkörper $k \subseteq K \subseteq L$. Zeige: Die Körpererweiterung $K \subseteq L$ erfüllt die Bedingungen in (a).

39. Sei p Primzahl, sei K ein Körper der Charakteristik p. Sei $K \subseteq L$ eine endliche Körpererweiterung und p sei kein Teiler von $[L : K]$. Zeige: L ist separabel über K.

40. Sei $K \subseteq L$ eine Körpererweiterung vom Grad n, sei $\alpha \in L$ und $L = K[\alpha]$. Ist die Charakteristik von K kein Teiler von n, so gibt es $\beta \in L$ mit $L = K[\beta]$, wobei das Minimalpolynom von β über K die Form $T^n + \sum_{i=0}^{n-2} c_i T^i$ mit $c_i \in K$ hat.

41. Sei K Körper, sei $f \in K[T]$ ein normiertes Polynom vom Grad n. Sei L der Zerfällungskörper von f über K. Zeige, daß $[L : K]$ ein Teiler von $n!$ ist.

Hinweis: Zeige zuerst: Sind $d_i \geq 1$ natürliche Zahlen $(1 \leq i \leq r)$, so ist $d_1!d_2! \cdots d_r!$ ein Teiler von $(d_1 + \cdots + d_r)!$.

10. Zerfällungskörper und Galois-Gruppen.

42. Sei $\alpha = \alpha_1 \in \mathbb{C}$ eine Wurzel des Polynoms $f = X^4 - 2X^2 + 2 \in \mathbb{Q}[X]$. (Hinweis: es gilt $(\alpha^2-1)^2 = -1$, man schreibt daher auch $\alpha = \sqrt{1+i}$ oder $\alpha = \sqrt{1-i}$). Zeige:

(a) Es sind auch $\alpha_2 = -\alpha,\ \alpha_3 = \overline{\alpha},\ \alpha_4 = -\overline{\alpha}$ Wurzeln von f (zeichne die Lage der vier Nullstellen in $\mathbb{C}$).

(b) Setze $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. Zeige $[L : \mathbb{Q}] = 8$. (Zum Beispiel kann man zeigen: $L = \mathbb{Q}(i)(\sqrt{2})(\alpha)$.)

(c) Versuche, alle Unterkörper von L zu konstruieren.

43. Bestimme $\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7}) : \mathbb{Q})$. Wie sehen demnach alle möglichen Zwischenkörper aus?

44. Sei

$$f = X^3 - 3X + 1 \in \mathbb{Q}[X].$$

Betrachte den Zerfällungskörper $L = \mathcal{Z}_{\mathbb{Q}}(f)$. Bestimme $[L : \mathbb{Q}]$. Wie sieht die Galois-Gruppe $\mathrm{Gal}(L : \mathbb{Q})$ aus?

45. Gegenbeispiel zur Aufgabe **32.**

(a) Sei $\alpha = e^{\frac{1}{4}\pi i} \in \mathbb{C}$. Zeige: Dies ist eine primitive achte Einheitswurzel und das Minimalpolynom über $\mathbb{Q}$ lautet $T^4 + 1$; das Polynom $f = T^4 + 1$ zerfällt über $\mathbb{Q}[\alpha]$ in Linearfaktoren, in $\mathbb{Q}$ gibt es aber keine primitive 4-te Einheitswurzel.

(b) Ist $p > 2$ eine beliebige Primzahl, kann man dann entsprechend einen endlichen Erweiterungskörper $\mathbb{Q} \subset \mathbb{Q}[\alpha]$ konstruieren, sodaß das Minimalpolynom von α die Form $f = T^p - a$ mit $a \in \mathbb{Q}$ hat und f über $\mathbb{Q}[\alpha]$ in Linearfaktoren zerfällt?

11.

46. Sei $f(X) = \sum_{i=0}^{n} a_i X_i$ ein normiertes Polynom vom Grad n mit Koeffizienten in $\mathbb{Z}$. Es gebe eine Primzahl p mit den folgenden Eigenschaften:

(i) p teilt alle Koeffizienten $a_0, a_1, \dots, a_{n-1}$.

(ii) p^2 ist kein Teiler von a_0.

Zeige: Das Polynom $f(X)$ ist irreduzibel in $\mathbb{Q}[X]$.

47. Beweise mit Hilfe von Aufgabe 46:

(a) Ist p eine Primzahl, und $n \geq 2$ eine natürliche Zahl, so ist $\sqrt[n]{p}$ keine rationale Zahl.

(b) Ist p eine Primzahl, so ist das Kreisteilungspolynom $\Phi_p(X)$ irreduzibel.

Hinweis zu (b): Betrachte statt $\Phi_p(X)$ das Polynom $\Phi_p(X+1)$.

Kreisteilungskörper

48. Sei ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$, mit $n = 5, 7, 11$. Bestimmen Sie alle Unterkörper von $\mathbb{Q}(\zeta)$.

49. Sei $\{\zeta_1, \dots, \zeta_n\}$ die Menge der n-ten Einheitswurzeln in $\mathbb{C}$, mit $n \in \mathbb{N}_1$. Beweise:

$$\zeta_1^k + \dots \zeta_n^k = \begin{cases} 0 & \text{falls } k \not\equiv 0 \pmod{n}, \\ n & \text{falls } k \equiv 0 \pmod{n}. \end{cases}$$

50. Sind m, n teilerfremde natürliche Zahlen, und ζ_m, ζ_n zugehörige primitive Einheitswurzeln, so gilt

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}.$$

12.

Zu bearbeiten sind (mindestens) **vier** der folgenden Aufgaben.

51. Man konstruiere die 5-ten Einheitswurzeln in $\mathbb{C}$ mit Zirkel und Lineal. (Verlangt ist: Zeichung mit Konstruktionsbeschreibung, Beweis). (Verwiesen sei hier auf die Aufgaben 29 und 30).

51* Für Mutige: Man konstruiere die 17-ten Einheitswurzeln in $\mathbb{C}$ mit Zirkel und Lineal.

52. "Konstruieren" bedeute auch hier: mit Zirkel und Lineal.

(a) Man zeige: Aus einem konstruierten regelmäßigen n-Eck kann man ein regelmäßiges $2n$-Eck konstruieren.

(b) Seien n_1, n_2 Zahlen mit $(n_1, n_2) = 1$. Hat man ein regelmäßiges n_1-Eck und ein regelmäßiges n_2-Eck konstruiert, so kann man auch ein regelmäßiges n_1n_2-Eck konstruieren.

(c) Für welche Zahlen $n \leq 100$ ist ein regelmäßiges n-Eck konstruierbar? (Beachte: die regelmäßigen n-Ecke mit $n = 3, 5$ und 17 sind konstruierbar).

53. Sei p Primzahl, $p-1 = md$ mit $m, d \in \mathbb{N}_1$. Sei ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Seien $\eta_0(d), \eta_1(d), \ldots, \eta_{m-1}(d)$ die d-gliedrigen Gauß'schen Perioden in $\mathbb{Q}[\zeta]$. Für $p = 7$ und $d = 2$ oder 3 soll berechnet werden:

(a) Die Multiplikationstabelle der $\eta_0(d), \eta_1(d), \ldots, \eta_{m-1}(d)$.

(b) Die Minimalpolynome von $\eta_0(d), \eta_1(d), \ldots, \eta_{m-1}(d)$ über $\mathbb{Q}$.

(c) Das Minimalpolynom von ζ über $\mathbb{Q}[\eta_0(d)]$.

54. Sei ζ eine primitive 12-te Einheitswurzel in $\mathbb{C}$. Wegen $\phi(12) = 4$ ist $G = \mathrm{Gal}(\mathbb{Q}[\zeta] : \mathbb{Q})$ eine Gruppe der Ordnung 4. Zeige: Dies ist die Klein'sche Vierergruppe. Bestimme alle Unterkörper von $\mathbb{Q}[\zeta]$.

Hinweis: Wie wir wissen, ist $G = \{g_1, g_5, g_7, g_{11}\}$, dabei ist g_a der Automorphismus von $\mathbb{Q}[\zeta]$ mit $g_a(\zeta) = \zeta^a$.

55. Sei $n \in \mathbb{N}_1$ und ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Bestimme alle Einheitswurzeln in $\mathbb{Q}[\zeta]$.

56. Seien $a, b \in \mathbb{Q}$. Betrachte das Polynom

$$f = X^4 + aX^2 + b \in \mathbb{Q}[X].$$

Sei L der Zerfällungskörper von f über $\mathbb{Q}$. Bestimme in Abhängigkeit von a, b den Grad $[L : \mathbb{Q}]$ und die Galois-Gruppe $\mathrm{Gal}(L : \mathbb{Q})$.