Proseminar Algebra und diskrete Mathematik

SS 2017

Bachelorstudium Lehramt Sekundarstufe (Allgemeinbildung)
Lehramtsstudium Unterrichtsfach Mathematik

Ganze Zahlen:

1. Zeigen Sie folgende Teibarkeiten ($n \in \mathbb{N}$):

   a.) $9|10^{33}+8$ b.) $6|10^{10}+14$
   c.) $72|10^{20}+8$ d.) $3|n^3-n$
   e.) $5|n^5-n$ f.) $7|n^7-n$
   g.) $11|n^{11}-n$ h.) $13|n^{13}-n$

   Gilt $9|n^9-n$?

2. Zeigen Sie dass folgende Zahlen zusammengesetzt sind:

   a.) 10^6-5^7 b.) $10^{100}-7$
   c.) $4^{20}-1$ d.) 1000027
   e.) $10^{300}-2\cdot 10^{100}+1$ f.) $1!+2+3!+\ldots+100!$
   g.) 347777743 h.) $4^9+6^{10}+3^{20}$
   i.) $2^{10}+5^{12}$ j.) $989\cdot 1001\cdot 1007+320$

3. Was ist die kleinste natürliche Zahl, die durch $1,2,3,4,5,6,7,8,9,10$ teilbar ist?
4. Zeigen Sie, dass die Summe von 9 aufeinanderfolgenden Zahlen immer durch 9 teilbar ist.
5. Zeigen Sie, dass die Summe von 10 aufeinanderfolgenden Zahlen nie durch 10 teilbar ist.
6. Wir multiplizieren 5 aufeinanderfolgende zahlen. Was ist die letzte Ziffer?
7. Wir multiplizieren 5 aufeinenderfolgende ungerade Zahlen. Was ist die letzte Ziffer?

Komplexe Zahlen:

8. Berechnen Sie die reellen Zahlen x und y so, dass es gilt

$$(1+2\mathrm{i})x+(3-5\mathrm{i})y=1-3\mathrm{i}.$$

9. Berechnen Sie die reellen Zahlen x, y, z und t so, dass es gilt

$$\begin{aligned}(1+\mathrm{i})x+(1+2\mathrm{i})y+(1+3\mathrm{i})z+(1+4\mathrm{i})t&=1+5\mathrm{i}\\(3-\mathrm{i})x+(4-2\mathrm{i})y+(1+i)z+4\mathrm{i}t&=2-\mathrm{i}.\end{aligned}$$

10. Berechnen Sie den Ausdruck i^n mit $n \in \mathbb{N}$.
11. Berechnen Sie den Ausdruck

$$(x-1-\mathrm{i})(x-1+i)(x+1+i)(x+1-\mathrm{i})=.$$

12. Berechnen Sie:

$$(1+2\mathrm{i})^6=?,\qquad (2+\mathrm{i})^7+(2-\mathrm{i})^7=?,\qquad (1+2\mathrm{i})^5-(1-2\mathrm{i})^5=?$$

13. Berechnen Sie ($a, b, \alpha \in \mathbb{R}$):

$$\frac{a+b\mathrm{i}}{a-b\mathrm{i}} =? \qquad \frac{(1+2\mathrm{i})^2-(1-\mathrm{i})^3}{(3+2\mathrm{i})^3-(2+\mathrm{i})^2} =?$$

$$\frac{(1-\mathrm{i})^5-1}{(1+\mathrm{i})^5+1} =? \qquad \frac{(1+\mathrm{i})^9}{(1-\mathrm{i})^7} =?$$

$$\frac{(1+\mathrm{i})^n}{(1+\mathrm{i})^{n-2}} =? \qquad \frac{1+\mathrm{i}\,\mathrm{tg}\,\alpha}{1-\mathrm{i}\,\mathrm{tg}\,\alpha} =?$$

14. Berechnen Sie:

$$\left(-\frac{1}{2}+\frac{\mathrm{i}\sqrt{3}}{2}\right)^2 =? \qquad \left(-\frac{1}{2}+\frac{\mathrm{i}\sqrt{3}}{2}\right)^3 =?$$

15. Lösen Sie:

a. $x^2-(2+\mathrm{i})x+(-1+7\mathrm{i})=0$

b. $x^2-(3-2\mathrm{i})x+(5-5\mathrm{i})=0$

c. $(2+\mathrm{i})x^2-(5-\mathrm{i})x+(2-2\mathrm{i})=0$

Polynome:

16. Multiplizieren Sie folgende Polynome:

a. $(2x^4-x^3+x^2+x+1)(x^2-3x+1) =?$

b. $(x^3+x^2-x-1)(x^2-2x-1) =?$

c. $(x^5+x^4+x^3+x^2+x+1)(x-1) =?$

17. Dividieren Sie mit Rest:

a. $(x^4-2x^3+4x^2-6x+8):(x-1)$

b. $(2x^5-5x^3-8x):(x+3)$

c. $(4x^3+x^2):(x+1+\mathrm{i})$

d. $(x^3-x^2-x):(x-1+2\mathrm{i})$

18. Was ist $a \in \mathbb{Z}$, falls ax^3+11x^2+7x+a durch $(2x+3)$ teilbar ist?

19. Was sind $a, b \in \mathbb{Z}$, falls $2x^4+5x^3-17x^2+ax+b$ durch $(2x^2-x-6)$ teilbar ist?

20. Zeigen Sie, dass $(x-2)^{100}+(x-1)^{50}-1$ durch (x^2-3x+2) teilbar ist.

21. Zerlegen Sie folgende Aurdrücke als Produkte von Polynomen mit ganzzahligen Koeffizienten!

a.) $x^4+x^3+2x^2+x+1$ b.) x^3+2x^2+2x+1

c.) $x^4+2x^3+2x^2+2x+1$ d.) $x^4+2x^3+3x^2+2x+1$

e.) x^4+x^2+1 f.) $x^{10}+x^8+x^6+x^4+x^2+1$

g.) x^4+4 h.) x^4-7x^2+1

1 Ganze Zahlen

„Es gibt 10 sorten von Menschen. Diejenigen, die wissen was die Binärdarstellung von Zahlen bedeutet, und diejenigen, die es nicht wissen."
„OCT 31 = DEC 25"

22. Schreiben Sie einen Programm, der natürliche Zahlen mit Rest dividiert.
23. Schreiben Sie einen Programm, der die Zifferndarstellung von natürlichen Zahlen zur Basis b berechnet.
24. Formulieren und beweisen Sie die Teilbarkeitsregeln mit 2,5, und 10 bezüglich die Zifferdarstellung zur Basis 10.
25. Formulieren und beweisen Sie die Teilbarkeitsregeln mit 3 und 9 bezüglich die Zifferdarstellung zur Basis 10.
26. Formulieren und beweisen Sie die Teilbarkeitsregeln mit 4 und 25 bezüglich die Zifferdarstellung zur Basis 10.
27. Formulieren und beweisen Sie die Teilbarkeitsregeln mit 8 und 125 bezüglich die Zifferdarstellung zur Basis 10.
28. Formulieren und beweisen Sie die Teilbarkeitsregeln mit 11 bezüglich die Zifferdarstellung zur Basis 10.
29. Zeigen Sie für $a, b, c \in \mathbb{N}$, $a \neq b$ dass es
$$ggT(a, b) = ggT(a - c \cdot b, b)$$
gilt.
30. Schreiben Sie einen Programm, der den größten gemeinsamen Teiler von zwei natürlichen Zahlen berechnet.
31. Beweisen Sie die Formel für das kleinste gemeinsame Vilfaches von $a, b \in \mathbb{N}$:
$$kgV(a, b) = \frac{a}{ggT(a, b)}b = \frac{b}{ggT(a, b)}a.$$
32. Seien $a, b \in \mathbb{N}$. Zeigen Sie, dass es ganze Zahlen $u, v \in \mathbb{Z}$ existieren so dass
$$u \cdot a + v \cdot b = ggT(a, b).$$
33. Sei M der Ring der geraden Zahlen. Welche Zahlen haben gar keinen Teiler in diesem Ring? Welche haben genau zwei (positive oder negative) Teiler?
34. Betrachten Sie den Ring der Zahlen
$$N := \{a + b\sqrt{2} \,:\, a, b \in \mathbb{Z}\}.$$
    (a) Ist $12 - 7\sqrt{2}$ durch $3 + 4\sqrt{2}$ teilbar?
    (b) Welche Zahlen sind durch $1 + \sqrt{2}$ teilbar?
    (c) Wir nennen eine Zahl, die jede Zahl teilt, eine Einheit. Wie viele Einheiten gibt es in diesem Ring?
35. Formulieren und beweisen Sie die Teilbarkeitsregeln mit 2 bezüglich die Zifferdarstellung zur Basis 9.
36. Formulieren und beweisen Sie die Teilbarkeitsregeln mit 3 bezüglich die Zifferdarstellung zur Basis 9. Was für andere Teilbarkeitsregeln können Sie bezüglich die Zifferdarstellung zur Basis 9 noch formulieren?
37. Betrachten Sie den Ring der gaußschen Zahlen
$$\mathbb{Z}[\mathrm{i}] := \{a + b\mathrm{i} \,:\, a, b \in \mathbb{Z}\}.$$
    (a) Ist $7 + \mathrm{i}$ durch $2 + \mathrm{i}$ teilbar?
    (b) Welche Zahlen sind durch $1 + \mathrm{i}$ teilbar?
    (c) Wir nennen eine Zahl, die jede Zahl teilt, eine Einheit. Wie viele Einheiten gibt es in diesem Ring?
    (d) Beweisen Sie: $\alpha|\beta \Leftrightarrow \bar{\alpha}|\bar{\beta}$.
    (e) Ist $5 \in \mathbb{Z}[i]$ eine Primzahl? Was ist mit 13? Und 11?

(f) Berechnen Sie $ggT(8+\mathrm{i}, 11-3\mathrm{i})$!

38. Eine natürliche Zahl n nennen wir *vollkommen*, wenn die Summe der echten (positiven) Teiler n zurückgibt. Zum Beispiel $6 = 1+2+3$ ist vollkommen. Zeigen Sie: wenn $2^{k+1}-1$ eine Primzahl ist, dann ist $n = 2^k(2^{k+1}-1)$ vollkommen. Geben Sie weitere Beispiele für vollkommene Zahlen.

39. (**Offene Probleme:**) Es ist nicht bekannt, ob es endlich viele oder unendlich viele vollkommene Zahlen gibt. Es ist auch nicht bekannt, ob es ungerade vollkommene Zahlen geben kann.

40. Zeigen Sie: ist n eine vollkommene Zahl, dann gilt

$$\sum_{k|n} \frac{1}{k} = 2.$$

41. (**Goldbachsche Vermutung: (offenes Problem)**) Jede gerade Zahl, die größer als 2 ist, ist Summe zweier Primzahlen.

42. Die sogenannte „schwache Goldbachsche Vermutung“ besagt, dass jede ungerade Zahl, die größer als 5 ist, ist Summe dreier Primzahlen. Zeigen Sie das diese Behauptung aus den Golbachschen Vermutung folgt. (Anmerkung: die schwache Goldbachsche Vermutung ist vor kurzem bewiesen worden.)

43. Sei p eine Primzahl und $a, b \in \mathbb{Z}$. Zeigen Sie: wenn p die Zahl $a \cdot b$ teilt, dann teilt p auch entweder a oder b.

44. Beweisen Sie dass jede (positive) ganze Zahl als Produkt von Primzahlen geschrieben werden kann.

45. Sei $H = \{p_1, p_2, \ldots, p_n\}$ eine Menge von Primzahlen. Zeigen Sie dass es eine Primzahl q geben muss, die nicht zu diese Menge gehört. Folgern Sie dass die Menge der Primzahlen unendlich sein muss.

46. Schreiben Sie einen Programm der die Primzahlen bis 10000 auflistet.

47. Sei p eine Primzahl und $a, b \in \mathbb{Z}_p$. Zeigen Sie dass der Traum von schlechten Schülern,

$$(a+b)^p = a^p + b^p$$

in $\mathbb{Z}_p$ gilt.

48. („kleiner Satz von Fermat“) Sei p eine Primzahl und $a \in \mathbb{Z}^p$. Zeigen Sie dass

$$a^p = a$$

in $\mathbb{Z}_p$ gilt.

49. Seien $a, m \in \mathbb{N}$. Zeigen Sie dass die Kongruenz

$$ax \equiv b \bmod (m)$$

genau dann lösbar ist wenn $ggT(a, m)|b$.

50. („Chinesischer Restsatz“, vermutlich 3. Jhd.): Seien $m_1, m_2 \in \mathbb{N}$ relativ prim (teilerfremd), und $a_1, a_2 \in \mathbb{N}$. Zeigen Sie dass die Kongruenzen

$$x \equiv a_1 \bmod (m_1)$$
$$x \equiv a_2 \bmod (m_2)$$

gleichzeitig lösbar sind.

51. Lesen Sie die Wikipedia-Seiten über „Primzahlzwilling“, „Terence Tao“, „Großer Fermatscher Satz“.

2 Polynome

Sei R ein Ring (z.B. $R = \mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C} \ldots$), $a_0, a_1, \ldots a_n \in R$, $a_n \neq 0$, und wir betrachten das Polynom

$$p(x) = \sum_{i=0}^{n} a_i x^i.$$

Wenn wir über x nichts sagen, dann ist $x \in \mathbb{C}$. Die Menge der Polynome bezeichnen wir mit $R[x]$.

Der „Fundamentalsatz der Algebra“besagt, dass ein komplexes Polynom immer mindestens eine (komplexe) Nullstelle hat, d.h., die Gleichung $p(x) = 0$ immer eine Lösung hat. Den Satz werden wir in der Analysis beweisen.

52. Leiten Sie eine Lösungsformel für die Gleichung $x^2 + px + q = 0$ her, wo $p, q \in \mathbb{C}$.
53. Leiten Sie eine Lösungsformel für die Gleichung $ax^2 + bx + c = 0$ mit $a, b, c \in \mathbb{C}$.
54. Zeigen Sie: Falls $a, b, c \in \mathbb{R}$, dann hat die Gleichung $ax^2 + bx + c = 0$ entweder reelle Lösungen, oder zwei komplexe, die zueinander konjugiert sind.
55. („Satz von Vieta (François Viète 1540–1603)“) Zeigen Sie: Sind x_1 und x_2 Lösungen von $x^2 + px + q = 0$, dann ist $x_1 + x_2 = -p$, $x_1 \cdot x_2 = q$.
56. Beweisen Sie: $x_0 \in \mathbb{C}$ ist genau dann eine Nullstelle des Polynoms $p(x)$, wenn $(x - x_0)|p(x)$. Allgemeiner, zeigen Sie dass falls $p(x)$ durch $(x - z)$ dividiert wird, ist der Rest r gleich $f(z)$.
57. Zeigen Sie, dass jedes komplexe Polynom sich als Produkt von linearen Polynomen schreiben lässt.
58. Zeigen Sie, dass jedes reelle Polynom sich als Produkt von linearen oder quadratischen reellen Polynomen schreiben lässt.
59. Sei x_0 eine „mehrfache Nullstelle“ von $p(x)$, das heißt $p(x) = (x - x_0)q(x)$ mit $q(x_0) = 0$. Die Ableitung von $p(x)$ definiert man wie üblich durch

    $$p'(x) = a_1 + 2a_2x + 3a_3x^2 + \ldots + na_nx^{n-1}.$$

    Zeigen Sie: x_0 ist genau dann eine mehrfache Nullstelle von $p(x)$, wenn x_0 eine Nullstelle von $p'(x)$ ist.
60. Verallgemeinern Sie den Satz von Vieta (Aufgabe 55) zur Polynome höherer (3., 4., n.) Ordnung.
61. („Cardano, Tartaglia, ... um 1530“) Wir wollen in dieser Aufgabe eine allgemeine Lösungsformel (ähnlich wie bei quadratischen Gleichungen) für die Gleichung $x^3 + px + q = 0$ herleiten.
    (a) Vergewissern Sie sich über die Identität $(u + v)^3 = 3uv(u + v) + (u^3 + v^3)$.
    (b) Das heißt $x = u + v$ ist eine Lösung, wenn $3uv = -p$ und $u^3 + v^3 = -q$ gilt. Lösen Sie also das Gleichungssytem

    $$27wz = -p^3$$
    $$w + z = -q.$$

    (c) Kombinieren Sie aus den vorigen Rechnungen eine Lösungsformel der Form

    $$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

    (d) Berechnen Sie was der Cardanischer Formel für die Gleichung $x^3 = 15x + 4$ liefert.
62. Führen Sie die Gleichung $x^3 + ax^2 + bx + c = 0$ auf eine Gleichung der Form $y^3 + py + q = 0$ zurück.
63. Lesen Sie Kapitel 3 „Biquadratische Gleichungen“ im Buch Bewersdorff: Algebra für Einsteiger.

64. Seien p und q polynome so dass es kein Polynom vom Grad ≥ 1 das sowohl p als auch q teilt (d.h. p und q sind *teilerfremd*), dann gibt es Polynome p^* und q^* so dass

$$p \cdot p^* + q \cdot q^* = 1.$$

(vergleiche mit Aufgabe 32)

65. Wir nennen ein Polynom $p \in R[x]$ irreduzibel, falls sein Grad mindestens 1 ist und jedes Polynom aus $R[x]$, das p teilt, entweder Grad 0 hat oder ein skalares Vielfaches von p ist. (Analog zu Primzahlen.) Bestimmen Sie die irreduziblen Polynome in $\mathbb{C}[x]$ und in $\mathbb{R}[x]$.

66. Zerlegen Sie die Polynome $x^4 + 1$, $x^4 + x^3 + x + 1$, $x^5 + 1$ aus $\mathbb{Z}_2[x]$ in irreduzible Polynome.

67. (Eisenstein)

    (a) Sei $p(x) = a_0 + a_1 x + a_2 x^2 \in \mathbb{Z}[x]$ und p eine Primzahl so dass $p \nmid a_2$, $p \mid a_0, a_1$ und $p^2 \nmid a_0$. Zeigen Sie dass p irreduzibel ist in $\mathbb{Z}[x]$.

    (b) Sei $p(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 \in \mathbb{Z}[x]$ und p eine Primzahl so dass $p \nmid a_3$, $p \mid a_0, a_1, a_2$ und $p^2 \nmid a_0$. Zeigen Sie dass p irreduzibei ist in $\mathbb{Z}[x]$.

    (c) Verallgemeinern Sie dies und formulieren Sie ein allgemeines Kriterium für Irreduzibilität in $\mathbb{Z}[x]$.

    (d) Überlegen Sie, dass $p(x) = 1 + x + x^2$ irreduzibel ist, aber dieses Kriterium nicht erfüllt.

68. Konstruieren Sie ein Polynom p vom Grad ≤ 1 so dass

    (a) $p(1) = 9$, $p(3) = 2$

    (b) $p(3) = 1$, $p(42) = 1$

69. Konstruieren Sie ein Polynom p vom Grad ≤ 2 so dass

    (a) $p(1) = 9$, $p(3) = 2$

    (b) $p(3) = 1$, $p(42) = 1$, $p(5) = 7$

    (c) $p(x_0) = y_0$, $p(x_1) = y_1$, $p(x_2) = y_2$

70. (Lagrangeinterpolation) Seien $x_0, x_1, x_2, y_0, y_1, y_2$ gegeben und Betrachten wir die Lagrange Polynome

$$l_0(x) = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2},\ l_1(x) = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2},\ l_0(x) = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1}.$$

    Zeigen Sie:

    (a) $l_i(x_j) = \delta_{ij}$ für $i, j = 0, 1, 2$.

    (b) Das Polynom $p(x) = y_0 l_0(x) + y_1 l_1(x) + y_2 l_2(x)$ erfüllt die Bedingung

$$p(x_i) = y_i, \qquad i = 0, 1, 2.$$

71. Konstruieren Sie ein Polynom p vom Grad ≤ 2 so dass

    (a) $p(1) = 9$, $p'(1) = 2$

    (b) $p(0) = 1$, $p'(0) = 1$, $p''(0) = 7$

    (c) $p(0) = y_0$, $p'(0) = y_1$, $p''(0) = y_2$ (Hermiteinterpolation)

72. Lesen Sie die Wikipedia-Seiten „Joseph-Louis Lagrange“ und „Charles Hermite“.

3 Gruppen

Eine Gruppe ist eine nichtleere Menge G mit einer Verknüpfung $\cdot$ so dass:
(i) Die Verknüpfung ist assoziativ, d.h., $f \cdot (g \cdot h) = (f \cdot g) \cdot h$ für alle $f, g, h \in G$.
(ii) Es gibt ein sogenanntes neutrales Element $e \in G$ so dass $e \cdot g = g$ für jedes $g \in G$.
(iii) Zu jedem $g \in G$ gibt es ein sogenanntes linksinverses Element $g^{-1} \in G$ so dass $g^{-1} \cdot g = e$.
Eine Gruppe heißt abelsch oder kommutativ, falls $g \cdot h = h \cdot g$ gilt für jedes $g, h \in G$.

73. Zeigen Sie, dass linksinverse Elemente auch rechtsinverse sind, d.h., $g \cdot g^{-1} = e$ gilt für jede $g \in G$.

74. Zeigen Sie, dass $g \cdot e = g$ gilt für jedes $g \in G$.

75. Zeigen Sie dass die neutrale Elemente und die Inverse eindeutig sind.

76. Listen Sie Beispiele von Gruppen auf. Geben Sie Beispiele für Mengen mit einer Verknüpfung, die keine Gruppe sind.

77. Zeigen Sie dass S_n und A_n, die symmetrische und die alternierende Gruppe eine Gruppe ist.

78. Überlegen Sie die Gruppeneigenschaft bei $GL(n)$, $O(n)$ und $SO(n)$.

79. Sei $U \subset G$ eine Untergruppe von G und betrachten wir die Nebenklassen $gU := \{g \cdot u \,|\, u \in U\}$. Zeigen Sie dass $gU = hU$ genau dann wenn $h^{-1}g \in U$.

80. Zeigen Sie dass unterschiedliche Nebenklassen disjunkt sind und gleich viele Elemente haben.

81. Wir nennen die Anzahl der Nebenklassen von G nach U den Index von U in G und bezeichnen mit $[G : U]$. Zeigen Sie den Satz von Lagrange:
$$|G| = |U| \cdot [G : U],$$
wo $|G|$ die Anzahl der Elemente der Gruppe G bezeichnet (und wird die Ordnung der Gruppe G genannt).

82. Die von $g \in G$ erzeugte Untergruppe bezeichnen wir mit $\langle g \rangle$ und die Ordnung von $\langle g \rangle$ nennen wir die Ordnung von g. Zeigen Sie dass die Ordnung von g immer $|G|$ teilt.

83. Zeigen Sie, dass die Ordnung von g die kleinste $k \in \mathbb{N}$ ist mit $g^k = e$.

84. Welche Elemente erzeugen $(\mathbb{Z}, +)$?

85. (Kleiner Satz von Fermat):
$$g^{|G|} = e.$$

86. Wir nennen eine Untergruppe $N \subset G$ Normalteiler, falls für alle $g \in G$ es gilt
$$g^{-1}Ng = N.$$
Zeigen Sie dass A_n ein Normalteiler ist in S_n und dass jede Untergruppe einer abelschen Gruppe ein Normalteiler ist.

87. Seien G, H Gruppen und $f : G \to H$ ein Homomorphismus von Gruppen. Zeigen Sie, dass $\ker(f)$ ein Normalteiler ist.

88. Sei N ein Normalteiler von G. Zeigen Sie, dass G/N, die Menge der Nebenklassen eine Gruppe ist (es heißt die Faktorgruppe) mit der Verknüpfung
$$(gN) \cdot (hN) = ghN.$$

89. (Homomorphiesatz für Gruppen): Sei $f : G \to H$ ein Homomorphismus der Gruppe G in die Gruppe H. Zeigen Sie, dass es
$$G/\ker(f) \cong \mathrm{Im}(f).$$

90. Bestimmen Sie die Symmetriegruppe des Quadrats, eines Rechtecks der kein Quadrat ist, und eines Würfels.

91. Bestimmen Sie die Symmetriegruppe eines regulären Tetraeders. Was ist die Ordnung dieser Gruppe?

92. Sei G eine Gruppe von Ordnung 65536. Zeigen Sie dass es ein Element der Ordnung 2 gibt.

4 Geometrische Konstruktionen

93. Überlegen Sie sich, was alles man mit Hilfe von Zirkel und Lineal konstruieren kann. Erklären Sie in Worten, wie Sie folgende Konstruktionen machen würden.

    (a) Konstruieren Sie eine Normale zu einer gegebenen Geraden durch einen gegebenen Punkt.

    (b) Konstruieren Sie eine Parallele zu einer gegebenen Geraden durch einen gegebenen Punkt.

    (c) Seien gegeben zwei sich in einem Punkt schneidende Geraden, konstruieren Sie eine winkelhalbierende Gerade.

    (d) Konstruieren Sie ein regelmäßiges Dreieck, Viereck und Fünfeck.

94. Gegeben ist eine Gerade mit zwei Punkten, 0 und 1. Wir nennen eine reelle Zahl α konstruierbar, wenn man mit Zirkel und Lineal eine Strecke mit Länge $|\alpha|$ konstruieren kann.

    (a) Zeigen Sie, dass $\mathbb{N}$ konstruierbar ist.

    (b) Ist a und b konstruierbar, zeigen Sie dass $a+b$, $a \cdot b$ und für $b \neq 0$ auch $\frac{1}{b}$ konstruierbar sind. Das heißt insbesondere, dass die konstruierbaren Zahlen einen Körper formen, und $\mathbb{Q}$ konstruierbar ist.

    (c) Ist $a > 0$ konstrueirbar, zeigen Sie dass auch $\sqrt{a}$ konstruierbar ist.

95. Sei $K_0 = \mathbb{Q}$, und für ein $d_1 \in \mathbb{Q}$ mit $\sqrt{d_1} \notin \mathbb{Q}$ definiere $K_1 = K_0[\sqrt{d_1}] := \{a + b\sqrt{d_1} : a, b \in K_0\}$, $K_2 := K_1[\sqrt{d_2}]$ für ein $d_2 \in K_1$ mit $\sqrt{d_2} \notin K_1$, usw., und $K_n := K_{n-1}[\sqrt{d_n}]$ für ein $d_n \in K_{n-1}$ mit $\sqrt{d_n} \notin K_{n-1}$.

    (a) Zeigen Sie, dass jedes K_i ein Körper ist und $\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \ldots \subsetneq K_n \subsetneq \mathbb{R}$.

    (b) Sei $\alpha \in \mathbb{R}$ so, dass es $n \in \mathbb{N}$ und Zahlen $d_1, \ldots d_n$ gibt, so dass $\alpha \in K_n$. Zeigen Sie, dass α konstruierbar ist.

    (c) Überlegen Sie: welche Gleichungen man lösen muss, wenn man die Koordinaten der Schnittpunkte
    - von zwei geraden,
    - von eine Gerade und einen Kreis, und
    - von zwei Kreise berechnen will?

    (d) Zeigen Sie, dass $\alpha \in \mathbb{R}$ genau dann konstruierbar ist, wenn es $n \in \mathbb{N}$ und Zahlen $d_1, \ldots d_n$ gibt, so dass $\alpha \in K_n$.

96. (Delisches Problem) Einer alten griechischen Sage zufolge wurde bei einem Orakelspruch zu Delos die Verdoppelung des Delischen Altarwürfels gefordert. Die Frage war also, wie kann man aus der vorhandenen Kantenlänge des Altarwürfels die Kantenlänge eines bezüglich des Volumens doppelt so großen Altarwürfels ermitteln? Beantworten Sie diese Frage, indem Sie zeigen, dass $\sqrt[3]{2}$ nicht konstruierbar ist. Dazu überlegen Sie folgendes.

    (a) Die Zahl $\sqrt[3]{2}$ ist irrational.

    (b) Gibt es $n \in \mathbb{N}$ und $d_1, \ldots d_n$ so dass $\sqrt[3]{2} \in K_n$, dann ist $\sqrt[3]{2} \in K_{n-1}$.

    (c) Fassen Sie das alles zusammen, und zeigen Sie, dass $\sqrt[3]{2}$ nicht konstruierbar ist.

97. (Winkeldreiteilung) Wir werden zeigen, dass es keine Konstruktion gibt mit dem man einen Winkel nur mit Zirkel und Lineal in drei gleiche Teile teilen kann. Wir werden uns dazu überlegen, dass der Winkel $20°$ nicht mit Zirkel und Lineal konstruierbar ist.

    (a) Überlegen Sie: Ein Winkel φ ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\cos\varphi$ und $\sin\varpi$ konstruierbare Zahlen sind.

    (b) Leiten Sie eine Formel für $\cos 3\varphi$ mit Hilfe von $\cos\varphi$ ab.

    (c) Zeigen Sie: falls $u = \cos 20°$, $x = 2u$, dann gilt $x^3 - 3x - 1 = 0$.

    (d) Zeigen Sie, dass falls $p(x) = x^3 - 3x - 1$ eine Nullstelle $a + b\sqrt{d} \in K_1 = K_0[d]$ hat, dann ist auch $a - b\sqrt{d}$ eine Nullstelle. Folgern Sie aus den Formeln von Vieta dass $x_3 \in K_0$.

    (e) Fassen Sie das alles zusammen und folgern Sie, dass $20°$ nicht mit Zirkel und Lineal konstruierbar ist.

98. Ist es möglich einen regelmäßigen 9-Eck mit Zirkel und Lineal zu konstruieren?

99. (Quadratur des Kreises) Zu einem gegebenen Kreis kann man kein flächengleiches Quadrat konstruieren. Man kann sogar mehr zeigen: wir werden bei Analysis sehen dass π nicht algebraisch ist. [hier kein Beweis]

5 Gruppen und Polynome

100. Sei D_3 (sog. Diedergruppe) die Gruppe der Kongruenzabbildungen des gleichseitigen Dreiecks, die aus folgende Transformationen besteht:

- die identische Abbildung e,
- die Drehung d um 120° um den Mittelpunkt des Dreiecks,
- die Drehung d^2 um 240° um den Mittelpunkt des Dreiecks,
- die drei Spiegelungen s_1 s_2 und s_3 an den drei Mittelsenkrechten des Dreiecks.

(a) Zeige, dass $D_3 \cong S_3$. Identifiziere die einzelne Kongruenzabbildungen mit Permutationen.

(b) Was sind die Untergruppen? Welche davon sind Normalteiler? Welche kann mit A_3 identifiziert werden?

Sei $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} + x^n = (x - x_1)(x - x_2)\cdots(x - x_n)$. Durch die Formeln von Vieta erhalten wir die sog. elementarsymmetrische Polynome:

$$\begin{aligned} a_{n-1} &= -(x_1 + x_2 + \ldots + x_n) = -\sum_{k=1}^{n} x_k \\ a_{n-2} &= x_1x_2 + x_1x_3 + \ldots x_{n-1}x_n = \sum_{\substack{i,j=1 \\ i<j}}^{n} x_ix_j \\ &\vdots \\ a_0 &= (-1)^n x_1x_2 \ldots x_n = \prod_{i=1}^{n} x_i. \end{aligned}$$

Sei $G \subset S_n$ eine Untergruppe. Eine funktion f von n Variablen heißt $G-$symmetrisch, falls für jede Permutation $\pi \in G$ es gilt

$$f(x_1, x_2, \ldots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}).$$

Ist $G = S_n$, dann heißt f einfach nur symmetrisch.

101. Betrachte für $n = 2$ die symmetrische Polynome $x_1^2 + x_2^2$, $x_1^3 + x_2^3$, $(x_1 - x_2)^2$. Kann man die mit Hilfe von a_0 und a_1 darstellen?

102. Betrachte für $n = 3$ die symmetrische Polynome $x_1^2 + x_2^2 + x_3^2$, $x_1^3 + x_2^3 + x_3^3$, $D_3 = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$. Kann man die mit Hilfe von a_0, a_1 und a_2 darstellen?

103. Gibt es eine Gruppe G so dass $\sqrt{D_3} = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ $G-$symmetrisch ist?

104. Überlegen Sie ob es stimmt dass jede symmetrische Polinom sich mit Hilfe von elementarsymmetrischen Polynomen darstellen lässt.

105. Sei $\zeta = -\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2}$ eine dritte Einheitswurzel und betrachte das Polynom $b_1 = \zeta x_1 + \zeta^2 x_2 + x_3$ und $b_2 = \zeta x_1 + \zeta^2 x_2 + x_3$. Zeige dass b_1^3 und b_2^3 symmetrisch sind. Kan man die mit Hilfe von a_0, a_1 und a_2 darstellen?

106. Seien $L \subset K$ zwei Körper. Die Galois-Gruppe der Körpererweiterung ist

$$Gal(K, L) = \{\varphi : K \to K \,|\, \varphi \text{ ist Körperautomorphismus mit } \varphi(x) = x \text{ für alle } x \in L\}.$$

Für ein Polynom p bezeichne mit $\mathbb{Q}(p)$ den Kleinsten Teikörper von $\mathbb{C}$ der alle Lösungen von $p(x) = 0$ enthält. Berechne $Gal(\mathbb{Q}(p), \mathbb{Q})$ für folgende Polynome:

(a) $p(x) = x^2 - a$,

(b) $p(x) = x^n - 1$.

107. Überlegen Sie dass die Galois-Gruppe $Gal(\mathbb{Q}(p), \mathbb{Q})$ immer eine Untergruppe von S_n ist.