Aufgabe 1. (4 Punkte)

Beweise mittels der Division mit Rest, dass jede Untergruppe H von $\mathbb{Z}$ die Gestalt $H = \mathbb{Z}d$ mit einem $d \in \mathbb{N}$ besitzt.

Lösung

Sei $H \subseteq \mathbb{Z}$ eine Untergruppe. Bei $H = 0$ kann man $d = 0$ nehmen, so dass wir voraussetzen dürfen, dass H neben 0 noch mindestens ein weiteres Element x enthält. Wenn x negativ ist, so muss die Untergruppe H auch das Negative davon, also $-x$ enthalten, welches positiv ist. D.h. H enthält auch positive Zahlen. Sei nun d die kleinste positive Zahl aus H. Wir behaupten $H = \mathbb{Z}d$. Dabei ist die Inklusion $\mathbb{Z}d \subseteq H$ klar, da mit d alle (positiven und negativen) Vielfache von d dazugehören müssen. Für die umgekehrte Inklusion sei $h \in H$ beliebig. Nach Division mit Rest gilt

$$h = qd + r \text{ mit } 0 \leq r < d\,.$$

Wegen $h \in H$ und $qd \in H$ ist auch $r = h - qd \in H$. Nach der Wahl von d muss wegen $r < d$ gelten: $r = 0$. Dies bedeutet $h = qd$ und damit $h \in \mathbb{Z}d$, also $H \subseteq \mathbb{Z}d$.

Aufgabe 2. (4 Punkte)

Es seien $n, m \in \mathbb{Z}$ ganze Zahlen. Zeige, dass n genau dann ein Teiler von m ist, wenn es einen Ringhomomorphismus

$$\mathbb{Z}/(m) \longrightarrow \mathbb{Z}/(n)$$

gibt. Zeige durch ein Beispiel, dass es einen injektiven Gruppenhomomorphismus

$$\mathbb{Z}/(m) \longrightarrow \mathbb{Z}/(n)$$

geben kann, ohne dass n ein Teiler von m ist.

Lösung

Wenn n ein Teiler von m ist, so ist $m = an$ und daher ist $m \in \mathbb{Z}n$ und somit gilt die Idealinklusion $\mathbb{Z}m \subseteq \mathbb{Z}n$. Unter dem kanonischen Ringhomomorphismus

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(n)$$

wird also $\mathbb{Z}m$ auf null abgebildet und daher gibt es nach dem Satz vom induzierten Homomorphismus einen Ringhomomorphismus

$$\mathbb{Z}/(m) \longrightarrow \mathbb{Z}/(n).$$

Wenn es umgekehrt einen solchen Ringhomomorphismus φ gibt, so betrachten wir insgesamt den Ringhomomorphismus

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(m) \xrightarrow{\varphi} \mathbb{Z}/(n)\,.$$

Die Gesamtabbildung muss also m auf null schicken, d.h. $m = 0 \mod n$, und m ist ein Vielfaches von n.

Für das Beispiel betrachten wir $n = 4$ und $m = 2$. In $\mathbb{Z}/(4)$ bildet die Menge $\{\bar{0}, \bar{2}\}$ eine Untergruppe, die zu $\mathbb{Z}/(2)$ isomorph ist, so dass ein injektiver Gruppenhomomorphismus $\mathbb{Z}/(2) \to \mathbb{Z}/(4)$ vorliegt.

Aufgabe 3. (3 Punkte)

(a) Bestimme für die Zahlen 2, 9 und 25 modulare Basislösungen, finde also die kleinsten positiven Zahlen, die in

$$\mathbb{Z}/(2) \times \mathbb{Z}/(9) \times \mathbb{Z}/(25)$$

die Restetupel $(1,0,0)$, $(0,1,0)$ und $(0,0,1)$ repräsentieren.

(b) Finde mit den Basislösungen die kleinste positive Lösung x der simultanen Kongruenzen

$$x = 0 \mod 2, x = 3 \mod 9 \text{ und } x = 5 \mod 25\,.$$

Lösung

(a) Modulare Basislösungen. Es ist $9 \times 25 = 225$, und dies hat modulo 2 den Rest 1. Es ist $2 \times 25 = 50$, und 50 hat modulo 9 den Rest 5, und 100 hat modulo 9 den Rest 1. Es ist $2 \times 9 = 18$. Wir gehen die Vielfachen von 18 durch und berechnen die Reste modulo 25:

$$18,\ 36 = 11,\ 54 = 4,\ 72 = 22,\ 90 = 15,\ 108 = 8,\ 126 = 1\,.$$

Die Basislösungen sind also $225, 100, 126$.

(b) Eine Lösung für die angegebenen simultanen Kongruenzen ist (modulo $2 \cdot 9 \cdot 25 = 450$)

$$0 \cdot 225 + 3 \cdot 100 + 5 \cdot 126 = 300 + 630 = 930 = 30\,.$$

Daher ist 30 die kleinste positive Lösung.

Aufgabe 4. (3 Punkte)

Wie viele Elemente besitzt die von der Drehung um 45 Grad, von der Drehung um 99 Grad und von der Zwölfteldrehung erzeugte Untergruppe der Drehgruppe SO_2?

Lösung

Wir schreiben die Drehungen als Teildrehungen einer Volldrehung, also

$$\frac{45}{360} = \frac{1}{8}, \frac{99}{360} = \frac{11}{40}, \frac{1}{12}.$$

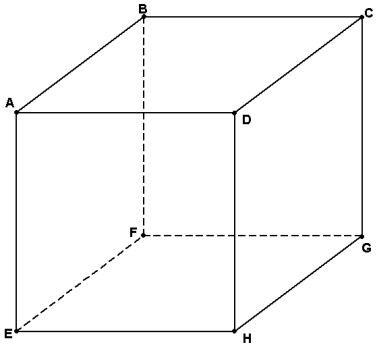
Mit dem Hauptnenner 120 sind dies die Drehungen

$$\frac{15}{120}, \frac{33}{120}, \frac{10}{120}.$$

Jede dieser Drehungen ist ein Vielfaches der $\frac{1}{120}$-Drehung. Andererseits sind die Zahlen $15, 33$ und 10 teilerfremd, so dass es eine Darstellung der 1 gibt. Daher ist die von den drei Drehungen erzeugte Untergruppe genau die von der $\frac{1}{120}$-Drehung erzeugte Untergruppe und enthält daher 120 Elemente.

Aufgabe 5. (6 Punkte)

Betrachte den Würfel



Es sei α diejenige Drehung am Würfel um die Achse durch die Eckpunkte A und G, die den Eckpunkt B auf D schickt, und es sei β die Halbdrehung um die vertikale Achse (also die Gerade, die durch den Mittelpunkt der Seitenfläche A, B, C, D und den Mittelpunkt der Seitenfläche E, F, G, H läuft).

a) Man gebe eine Wertetabelle für die Permutationen auf der Eckpunktmenge $\{A, B, C, D, E, F, G, H\}$, die durch $\alpha, \beta, \alpha\beta$ und $\beta\alpha$ bewirkt werden.

b) Bestimme die Drehachsen von $\alpha\beta$ und von $\beta\alpha$ sowie die Ordnung dieser Drehungen.

c) Man gebe die Zykeldarstellung der von α^2 bewirkten Permutation auf der Eckpunktmenge an. Was ist α^{1001}?

d) Man betrachte die Permutation σ, die auf der Eckpunktmenge durch die Wertetabelle

x	A	B	C	D	E	F	G	H
$\sigma(x)$	B	C	D	A	G	H	E	F

gegeben ist. Gibt es eine Drehung des Würfels, die diese Permutation bewirkt? Berechne das Signum von σ.

Lösung

a) Die Wertetabellen für die angegebenen Permutationen sind

x	A	B	C	D	E	F	G	H
$\alpha(x)$	A	D	H	E	B	C	G	F

x	A	B	C	D	E	F	G	H
$\beta(x)$	C	D	A	B	G	H	E	F

x	A	B	C	D	E	F	G	H
$\alpha\beta(x)$	H	E	A	D	G	F	B	C

x	A	B	C	D	E	F	G	H
$\beta\alpha(x)$	C	B	F	G	D	A	E	H

b) Die Drehachse von $\alpha\beta$ ist die Gerade durch die beiden Eckpunkte D und F und die Drehachse von $\beta\alpha$ ist die Gerade durch die beiden Eckpunkte B und H. Beides sind Dritteldrehungen, ihre Ordnung ist 3.

c) Aus der Wertetabelle für α kann man leicht diejenige für α^2 errechnen, und damit auch die Zykeldarstellung. Diese ist

$$\langle B, E, D\rangle\langle C, F, H\rangle\,.$$

α hat die Ordnung drei, daher ist $\alpha^{1001} = \alpha^2$.

d) σ stimmt auf den unteren Eckpunkten E, F, G, H mit der durch β definierten Permutation überein. Würde σ von einer Würfelbewegung γ herrühren, so wäre $\beta\gamma^{-1}$ die Identität auf der unteren Ebenen und müßte dann überhaupt die Identität sein. Dann wäre $\beta = \gamma$, was aber wegen

$$\beta(A) = C \neq B = \gamma(A)$$

nicht der Fall ist.

σ hat die Zykeldarstellung

$$\sigma = \langle A, B, C, D\rangle\langle E, G\rangle\langle H, F\rangle\,,$$

die wir als Produktdarstellung lesen. Der vordere Zykel ist als Produkt geschrieben

$$\langle A, B, C, D\rangle = \langle B, C\rangle\langle C, D\rangle\langle D, A\rangle\,.$$

Insgesamt ist σ das Produkt von 5 Transpositionen und daher ist das Signum -1.

Aufgabe 6. (3 Punkte)

Es sei R ein kommutativer Ring und $f \in R$. Charakterisiere mit Hilfe der Multiplikationsabbildung

$$\mu_f : R \longrightarrow R,\ g \longmapsto fg,$$

wann f ein Nichtnullteiler und wann f eine Einheit ist.

Lösung

Die Multiplikationsabbildung ist ein Gruppenhomomorphismus, wie direkt aus dem Distributivitätsgesetz folgt. Es gilt:

f ist ein Nichtnullteiler genau dann, wenn für alle $g \in R$ aus $fg = 0$ folgt $g = 0$. Dies ist genau dann der Fall, wenn der Kern von μ_f nur aus 0 besteht, was genau dann gilt, wenn μ_f injektiv ist.

f ist eine Einheit genau dann, wenn es ein $g \in R$ gibt mit $fg = 1$, was genau dann der Fall ist, wenn 1 zum Bild von μ_f gehört. Dies wiederum ist äquivalent dazu, dass μ_f surjektiv ist, denn aus $fg = 1$ folgt sofort $h = (fg)h = f(gh)$ für jedes $h \in R$.

Die nächste Aufgabe verwendet die folgende Definition.

Ein kommutativer Ring R heißt *angeordnet*, wenn es eine *totale Ordnung* „$\geq$“ auf R gibt, die die beiden Eigenschaften

(1) Aus $a \geq b$ folgt $a + c \geq b + c$ für beliebige $a, b, c \in R$.
(2) Aus $a \geq b$ folgt $ac \geq bc$ für beliebige $a, b, c \in R$ mit $c \geq 0$.

erfüllt.

Die Schreibweise $a > b$ bedeutet $a \geq b$ und $a \neq b$.

Aufgabe 7. (10 Punkte)

Es sei R ein angeordneter Integritätsbereich.

a) Zeige, dass aus $ca \geq cb$ mit $c > 0$ folgt, dass $a \geq b$ ist $(a, b, c \in R)$.

b) Zeige, dass $1 > 0$ in R gilt.

c) Zeige, dass aus $a > 0$ die Eigenschaft $-a < 0$ folgt.

d) Sei $K = Q(R)$ der Quotientenkörper von R. Definiere eine Ordnungsrelation $\geq$ auf K, die auf $R \subseteq K$ mit der vorgegebenen Ordnung übereinstimmt, und die K zu einem angeordneten Körper macht (Tipp: es empfiehlt sich, die Nenner positiv anzusetzen).

Lösung

a) Angenommen, unter den angegebenen Voraussetzungen wäre nicht $a \geq b$. Da eine totale Ordnung vorliegt, ist dann $a < b$. D.h. insbesondere $a \leq b$ und daraus folgt $ac \leq bc$. Wenn dies gleich wäre, würde wegen der Kürzbarkeit in einem Integritätsbereich und wegen $c \neq 0$ sofort $a = b$ folgen, was ausgeschlossen ist. Daher ist $ac < bc$ im Widerspruch zur Voraussetzung.

b) Die Eigenschaft $1 > 0$ ist aufgrund der ersten Eigenschaft äquivalent zu $0 > -1$, so dass wir $-1 \geq 0$ annehmen. Aufgrund der zweiten Eigenschaft ist dann $1 = (-1)(-1) \geq (-1)0 = 0$ und wegen $1 \neq 0$ in einem Integritätsbereich folgt doch $1 > 0$.

c) Aus $a < 0$ folgt durch beidseitige Addition mit $-a$ sofort $0 \leq -a$. Würde $0 = -a$ gelten, so folgt $a = 0$ im Widerspruch zur Voraussetzung, also ist $0 < -a$.

d) Ein Element im Quotientenkörper $K = Q(R)$ wird repräsentiert durch einen Bruch $\frac{a}{b}$ mit $a, b \in R$, $b \neq 0$ Dabei ist $\frac{a}{b} = \frac{c}{d}$ definitionsgemäß genau dann, wenn $ad = bc$ ist. Da eine totale Ordnung vorliegt, kann man stets annehmen, dass die Nenner positiv sind, da man mit -1 erweitern kann (nach Teil (c)). Im Folgenden nehmen wir alle Nenner als positiv an. Wir definieren

$$\frac{a}{b} \leq \frac{c}{d} \text{ wenn } ad \leq cb\,.$$

Man muss die Wohldefiniertheit dieser Definition nachweisen und dass die Eigenschaften eines geordneten Ringes erfüllt sind. Zur Wohldefiniertheit sei

$$\frac{a}{b} \leq \frac{c}{d}$$

und

$$\frac{a}{b} = \frac{a'}{b'} \text{ und } \frac{c}{d} = \frac{c'}{d'}\,.$$

Dann ist

$$a'd'cb = adb'c'.$$

Bei $c > 0$ ist

$$a'd'cb = adb'c' \leq c'b'cb$$

und daraus folgt durch kürzen (nach Teil (a)) $a'd' \leq c'b'$ wie gewünscht. Bei $c = 0$ ist auch $c' = 0$ und $\frac{a}{b} \leq 0$ bedeutet $a \leq 0$ und damit muss auch $a' \leq 0$ und $a'd' \leq 0$ sein. Bei $c < 0$ ist auch $c' < 0$. Dann ist $b'c' < 0$ und $-b'c' > 0$, also

$$a'd'(-cb) = ad(-b'c') \leq c'b'(-cb).$$

Daraus ergibt sich $a'd' \leq c'b'$. Daher ist die Ordnung wohldefiniert.

Jetzt sind die Ordnungseigenschaften zu testen. Es seien $x = \frac{a}{b}$, $y = \frac{c}{d}$ und $z = \frac{e}{f}$. Wir können stets zu einem Hauptnenner übergehen, also $b = d = f > 0$ annehmen. Aus dem bisher Bewiesenen folgt, dass $\frac{a}{b} \geq \frac{c}{b}$ genau dann gilt, wenn $a \geq c$ ist.

Die Reflexivität ist trivial. Zur Transitivität sei $x = \frac{a}{b} \leq y = \frac{c}{b}$ und $y = \frac{c}{b} \leq z = \frac{e}{b}$. Also ist $a \leq c$ und $c \leq e$ und daher ist $a \leq e$ und somit auch $x \leq z$.

Zur Antisymmetrie sei $\frac{a}{b} \leq \frac{c}{b}$ und $\frac{a}{b} \geq \frac{c}{b}$. Dann ist direkt $a = c$ und die Brüche stimmen überein.

Wir kommen nun zu den Eigenschaften eines geordneten Ringes.

(1). Aus $x = \frac{a}{b} \geq y = \frac{c}{b}$ folgt sofort $a \geq c$. Daher ist $a + e \geq c + e$ und somit wiederum

$$x + z = \frac{a+e}{b} \geq \frac{c+e}{b} = y + z.$$

(2). Sei $x \geq y$ und $z \geq 0$. Dann ist $a \geq c$ und $e \geq 0$ und somit $ae \geq ce$. Also ist

$$xz = \frac{a}{b}\frac{e}{b} = \frac{ae}{b^2} \geq \frac{ce}{b^2} = \frac{c}{b}\frac{e}{b} = yz.$$

Es ist trivial, dass eine Fortsetzung der Ordnung und eine totale Ordnung vorliegt.

Aufgabe 8. (5 Punkte)

Bestimme die Primfaktorzerlegung des Polynoms $X^6 - 1$ über den Körpern $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/(7)$ und $\mathbb{Z}/(5)$.

Lösung

Es ist (über jedem Körper)

$$\begin{aligned} X^6 - 1 &= (X^2 - 1)(X^4 + X^2 + 1) \\ &= (X - 1)(X + 1)(X^4 + X^2 + 1) \\ &= (X - 1)(X + 1)(X^2 + X + 1)(X^2 - X + 1). \end{aligned}$$

Dies kann man direkt bestätigen, es ergibt sich aber auch aus der Produktzerlegung von $X^6 - 1$ mit Hilfe der Kreisteilungspolynome. Über den komplexen Zahlen ist

$$X^6 - 1 = \prod_{k=0}^{5} (X - e^{\frac{2\pi i k}{6}}) .$$

Da davon vier Nullstellen imaginär sind, müssen die beiden quadratischen Polynome von oben über $\mathbb{Q}$ und über $\mathbb{R}$ irreduzibel sein, so dass die obige Faktorzerlegung über diesen Körpern die Primfaktorzerlegung ist. Über $\mathbb{Z}/(7)$ gilt aufgrund des kleinen Fermat für jede Einheit $x^6 = 1$. Daher ist die Faktorzerlegung

$$X^6 - 1 = (X - 1)(X - 2)(X - 3)(X - 4)(X - 5)(X - 6) .$$

Über $\mathbb{Z}/(5)$ haben die beiden Polynome $X^2 + X + 1$ und $X^2 - X + 1$ keine Nullstelle, sind also irreduzibel, und daher ist die obige Zerlegung auch die Primfaktorzerlegung über $\mathbb{Z}/(5)$.

Aufgabe 9. (3 Punkte)

Betrachte den Körper $K = \mathbb{F}_4 = (\mathbb{Z}/(2))[U]/(U^2 + U + 1)$. Führe im Polynomring $K[X]$ die Polynomdivision

$$X^4 + uX^3 + (u+1)X + 1 \text{ durch } uX^2 + X + u + 1$$

aus, wobei u die Restklasse von U in K bezeichnet.

Lösung

Die Division mit Rest ergibt

$X^4+uX^3+(u+1)X+1 = (uX^2+X+u+1)((u+1)X^2+(u+1)X+(u+1))+uX+u+1\,.$

Aufgabe 10. (6 Punkte)

Sei $\mathbb{F}_q$ ein endlicher Körper der Charakeristik ungleich 2. Zeige unter Verwendung der Isomorphiesätze, dass genau die Hälfte der Elemente aus $\mathbb{F}_q^\times$ ein Quadrat in $\mathbb{F}_q$ ist.

Lösung

Wir betrachten die Abbildung

$$\mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times,\, x \longmapsto x^2,$$

der Einheitengruppe in sich. Diese schickt 1 auf 1 und wegen $(xy)^2 = x^2y^2$ handelt es sich um einen Gruppenhomomorphismus. Der Kern dieser Abbildung besteht aus den $x \in \mathbb{F}_q^\times$ mit $x^2 = 1$, also aus den Nullstellen des Polynoms $X^2 - 1$. Dessen Nullstellen sind gerade 1 und -1, weitere Nullstellen kann es nicht geben, da die Anzahl der Nullstellen durch den Grad des Polynoms beschränkt ist. Bei $1 = -1$ wäre $2 = 0$, was aufgrund der Charakteristik ausgeschlossen ist. Also besteht der Kern genau aus zwei Elementen. nach dem Isomorphiesatz ist das Bild isomorph zum Urbild modulo Kern. Das Bild ist genau die Menge der Quadrate in der Einheitengruppe, und diese ist isomorph zu $\mathbb{F}_q^\times/\{+1, -1\}$. Jede Nebenklasse besitzt daher zwei Elemente und die Anzahl der Nebenklassen ist daher $\frac{q-1}{2}$. Die Hälfte der Einheiten sind also Quadrate.

Aufgabe 11. (4 Punkte)

Beschreibe den Körper mit neun Elementen $\mathbb{F}_9$ als einen Restklassenkörper von $\mathbb{Z}/(3)[X]$. Man gebe eine primitive Einheit in $\mathbb{F}_9$ an.

Lösung

In $\mathbb{Z}/(3)$ ist 2 kein Quadrat, wie man direkt nachrechnet. Daher ist $X^2-2 = X^2+1 \in \mathbb{Z}/(3)[X]$ ein irreduzibles Polynom und daher ist der Restklassenring

$$\mathbb{Z}/(3)[X]/(X^2+1)$$

ein Körper. Jedes Element wird dabei eindeutig geschrieben in der Form $ax+b$ (x bezeichnet die Restklasse von X) mit $a,b \in \mathbb{Z}/(3)$, so dass es sich um einen Körper mit 9 Elementen handelt.

Die Einheitengruppe von diesem Körper besitzt 8 Elemente. Alle Elemente haben also eine Zweierpotenz als Ordnung, und wir brauchen ein Element der Ordnung 8. Wir betrachten das Element $x+1$. Es ist

$$(x+1)^2 = x^2+2x+1 = 2x+3 = 2x \neq 1$$

und

$$(2x)^2 = 4x^2 = x^2 = 2 \neq 1.$$

Daher ist die Ordnung von $x+1$ weder 1 noch 2 noch 4, also muss sie gleich 8 sein und es liegt ein primitives Element vor.

Aufgabe 12. (3 Punkte)

Schreibe den Restklassenring $\mathbb{Q}[X]/(X^4-1)$ als ein Produkt von Körpern, wobei lediglich die Körper $\mathbb{Q}$ und $\mathbb{Q}[i]$ vorkommen dürfen. Schreibe die Restklasse von X^3+X als ein Tupel in dieser Produktzerlegung.

Lösung

Es ist $X^4-1=(X^2-1)(X^2+1)=(X+1)(X-1)(X^2+1)$ und $X^2+1\in\mathbb{Q}[X]$ ist irreduzibel, da es keine rationale Nullstelle besitzt. Es handelt sich also um die Primfaktorzerlegung, wobei die Faktoren paarweise nicht assoziiert sind, da sie ja alle normiert sind. Nach dem chinesischen Restsatz für Hauptidealbereiche gilt daher die Produktzerlegung

$$\mathbb{Q}[X]/(X^4-1)\cong\mathbb{Q}[X]/(X+1)\times\mathbb{Q}[X]/(X-1)\times\mathbb{Q}[X]/(X^2+1)\cong\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}[i],$$

wobei wir für das zweite Gleichheitszeichen die Einsetzungen $X\mapsto -1$ und $X\mapsto 1$ und die Isomorphie $\mathbb{Q}[X]/(X^2+1)\cong\mathbb{Q}[i]$ verwendet haben. Das Element $X^3+X=X(X^2+1)$ wird unter den drei Projektionen auf $-2,2$ und 0 abgebildet, es ist also gleich

$$(-2,2,0)\,.$$

Aufgabe 13. (5 Punkte)

Formuliere und beweise die „Gradformel“ für eine Folge von endlichen Körpererweiterungen $K \subseteq L \subseteq M$.

Lösung

Die Gradformel besagt

$$\operatorname{grad}_K M = (\operatorname{grad}_K L)(\operatorname{grad}_L M)\,.$$

Wir setzen $\operatorname{grad}_K L = n$ und $\operatorname{grad}_L M = m$. Es sei $x_1, \ldots, x_n \in L$ eine K-Basis von L und $y_1, \ldots, y_m \in M$ eine L-Basis von M. Wir behaupten, dass die Produkte

$$x_i y_j, 1 \leq i \leq n, 1 \leq j \leq m,$$

eine K-Basis von M bilden. Wir zeigen zuerst, dass diese Produkte den Vektorraum M über K aufspannen. Sei dazu $z \in M$. Wir schreiben

$$z = b_1 y_1 + \ldots + b_m y_m \text{ mit Koeffizienten } b_j \in L.$$

Wir können jedes b_j als $b_j = a_{1j} x_1 + \ldots + a_{nj} x_n$ mit Koeffizienten $a_{ij} \in K$ ausdrücken. Das ergibt

$$\begin{aligned} z &= b_1 y_1 + \ldots + b_m y_m \\ &= (a_{11} x_1 + \ldots + a_{n1} x_n) y_1 + \ldots + (a_{1m} x_1 + \ldots + a_{nm} x_n) y_m \\ &= \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} a_{ij} x_i y_j. \end{aligned}$$

Daher ist z eine K-Linearkombination der Produkte $x_i y_j$. Um zu zeigen, dass diese Produkte linear unabhängig sind, sei

$$0 = \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} c_{ij} x_i y_j$$

angenommen mit $c_{ij} \in K$. Wir schreiben dies als $0 = \sum_{j=1}^{m} (\sum_{i=1}^{n} c_{ij} x_i) y_j$. Da die y_j linear unabhängig über L sind und die Koeffizienten der y_j zu L gehören folgt, dass $\sum_{i=1}^{n} c_{ij} x_i = 0$ ist für jedes j. Da die x_i linear unabhängig über K sind und $c_{ij} \in K$ ist folgt, dass $c_{ij} = 0$ ist für alle i, j.

Aufgabe 14. (3 Punkte)

Es seien zwei verschiedene Punkte M, P in der Ebene gegeben. Es bezeichne K den Kreis mit Mittelpunkt M durch den Punkt P. Konstruiere (ohne andere Konstruktionen zu verwenden) die Tangente an den Kreis K durch P. Skizziere die Situation.

Lösung

Wir zeichnen den Kreis C mit Mittelpunkt P durch den Punkt M. Die Verbindungsgerade G durch M und P hat mit C (neben M) noch einen weiteren Schnittpunkt, den wir mit S bezeichnen. Wir zeichnen Kreise K_1 und K_2 mit Mittelpunkt S durch M und mit Mittelpunkt M durch S. Die beiden Schnittpunkte von K_1 und K_2 definieren eine Gerade H, und diese verläuft durch P und steht senkrecht auf G (H ist die halbierende Senkrechte der Strecke von M nach S), so dass H die Tangente an P ist.

Aufgabe 15. (2 Punkte)

Charakterisiere mit Hilfe von Fermatschen Primzahlen (ohne Beweis) diejenigen natürlichen Zahlen n, für die das reguläre n-Eck konstruierbar ist. Wende diese Charakterisierung für n zwischen 30 und 40 an.

Lösung

Zu einer natürlichen Zahl n ist das reguläre n-Eck genau dann konstruierbar, wenn die Primfaktorzerlegung von n die Gestalt hat

$$n = 2^{\alpha} p_1 \cdots p_k$$

mit verschiedenen Fermatsche Primzahlen $p_1, \ldots, p_k$. Dabei ist eine Fermatsche Primzahl eine Primzahl der Form $p = 2^s + 1$. Für das Zahlenintervall von 30 bis 40 sind nur die Fermatschen Primzahlen $3, 5, 17$ relevant, und daher sind lediglich die regulären n-Ecke für

$$30 = 2 \cdot 3 \cdot 5,\ 32 = 2^5,\ 34 = 2 \cdot 17,\ 40 = 2^3 \cdot 5$$

konstruierbar.