5.4. Quadratische Formen.

Seien $X_1, \ldots, X_n$ Variablen. Ein Produkt $X_1^{d_1} X_2^{d_2} \cdots X_n^{d_n}$ mit $\sum d_i = m$ nennt man ein *Monom vom Grad* m. Polynome sind (endliche!) Linearkombinationen von Monomen mit Koeffizienten in einem kommutativen Ring R.

Ein Polynom $f(x_1, \ldots, x_n)$ in n Variablen mit Koeffizienten im kommutativen Ring R heißt *m-Form,* falls höchstens die Koeffizienten der Monome vom Grad m von Null verschieden sind; statt 1-Form sagt man *Linearform*, statt 2-Form *quadratische Form.* Beispiel: Eine quadratische Form in 2 Variablen sieht folgendermaßen aus:

$$\alpha X^2 + \beta XY + \gamma Y^2,$$

mit $\alpha, \beta, \gamma \in R$. Ist eine m-Form f in n Variablen gegeben, so ist man immer an folgenden Fragen interessiert:

(1) Welche Werte werden angenommen? Wie sieht also die Menge

$$\{f(x_1, \ldots, x_n) \mid [x_1, \ldots, x_n] \in R^n\}$$

aus?

(2) Für welche n-Tupel $[x_1, \ldots, x_n] \in R^n$ gilt $f(x_1, \ldots, x_n) = 0$? Insbesondere: Gibt es unendlich viele solche n-Tupel? Oder nur endlich viele? Oder nur die triviale Null-Lösung ($[x_1, \ldots, x_n] = 0$, d.h.: alle $x_i = 0$). Hier wird also die Menge

$$\{[x_1, \ldots, x_n] \in R^n \mid f(x_1, \ldots, x_n) = 0\}$$

untersucht.

Natürlich kann man allgemeiner für jedes $r \in R$ die Menge

$$f^{-1}(r) = \{[x_1, \ldots, x_n] \in R^n \mid f(x_1, \ldots, x_n) = r\}$$

analysieren — die Frage (2) ist der Spezialfall $r = 0$, bei der Frage (1) dreht es sich darum, alle r zu bestimmen, für die diese Menge $f^{-1}(r)$ nicht leer ist.

Die Gleichung $\alpha x^2 + \beta y^2 + \gamma z^2 = 0$.

5.4.1. Satz (Legendre). *Seien $\alpha, \beta, \gamma \in \mathbb{Z} \setminus \{0\}$, und sei $\alpha\beta\gamma$ quadratfrei. Dann sind die folgenden Aussagen äquivalent:*

(1) *Es gibt ein von Null verschiedenes Tripel $[x, y, z]$ mit $\alpha x^2 + \beta y^2 + \gamma z^2 = 0$.*

(2) *Die Zahlen α, β, γ haben nicht das gleiche Vorzeichen und es gilt:*
$-\beta\gamma$ ist quadratischer Rest modulo α,
$-\gamma\alpha$ ist quadratischer Rest modulo β,
$-\alpha\beta$ ist quadratischer Rest modulo γ.

Beweis (Mordell, siehe NZ): Beachte: Da $\alpha\beta\gamma$ quadratfrei ist, sind die Zahlen α, β, γ paarweise teilerfremd.

(1) $\Longrightarrow$ (2). Sei $[x,y,z] \neq 0$ mit $\alpha x^2 + \beta y^2 + \gamma z^2 = 0$. Natürlich können α, β, γ nicht das gleiche Vorzeichen haben! Zu zeigen sind also nur die weiteren Aussagen.

Wir können voraussetzen, dass 1 der größte gemeinsame Teiler von x, y, z ist (sonst teilen wir x, y, z durch den größten gemeinsamen Teiler und erhalten ebenfalls eine Lösung). Wir zeigen: $(x, \gamma) = 1$. Ist nämlich p eine Primzahl, die x und γ teilt, so teilt p auch βy^2. Wegen $(\beta, \gamma) = 1$ sieht man, dass p ein Teiler von y ist, also ist p^2 ein Teiler von $\alpha x^2 + \beta y^2 = -\gamma z^2$. Da γ quadratfrei ist, folgt $p|z$, aber wir setzen voraus, dass x, y, z keinen gemeinsamen Primteiler haben.

Aus $(x, \gamma) = 1$ folgt, dass es ein $u \in \mathbb{Z}$ gibt mit $xu \equiv 1 \mod \gamma$. Wir rechnen modulo γ. Es ist

$$\alpha x^2 + \beta y^2 \equiv \alpha x^2 + \beta y^2 + \gamma z^2 = 0 \mod \gamma.$$

Wir multiplizieren dies mit βu^2 und erhalten

$$\alpha\beta x^2 u^2 + \beta^2 y^2 u^2 \equiv 0 \mod \gamma,$$

Also

$$-\alpha\beta \equiv -\alpha\beta x^2 u^2 \equiv (\beta y u)^2 \mod \gamma.$$

Analog sieht man, dass auch $-\beta\gamma$ Quadrat modulo α und $-\gamma\alpha$ Quadrat modulo β ist.

(2) $\Longrightarrow$ (1). Wir zeigen als erstes, dass $f = \alpha X^2 + \beta Y^2 + \gamma Z^2$ modulo γ Produkt zweier Linearformen ist. Sei $r \in \mathbb{Z}$ mit $r^2 \equiv -\alpha\beta$ modulo γ. Da (α, γ) teilerfremd sind, gibt es α' mit $\alpha\alpha' \equiv 1 \mod \gamma$. Modulo γ gilt dann:

$$\begin{aligned} \alpha x^2 + \beta y^2 + \gamma z^2 &\equiv \alpha x^2 + \beta y^2 \\ &\equiv \alpha\alpha'(\alpha x^2 + \beta y^2) = \alpha'(\alpha^2 x^2 + \alpha\beta y^2) \\ &\equiv \alpha'(\alpha^2 x^2 - r^2 y^2) = \alpha'(\alpha x + ry)(\alpha x - ry) \\ &\equiv (x + \alpha r y)(\alpha x - ry) \mod \gamma \end{aligned}$$

Entsprechend sieht man, dass f sowohl modulo α, als auch modulo β jeweils Produkt zweier Linearformen ist. Nun folgt aber ganz allgemein aus dem chinesischen Restsatz:

Lemma 1. *Sei $(n, m) = 1$. Lässt sich eine quadratische Form modulo n und auch modulo m als Produkt jeweils zweier Linearformen schreiben, so gilt das gleiche auch modulo nm.*

Beweis: Sei

$$\begin{aligned} f &\equiv (\sum \alpha'_i X_i)(\sum \beta'_i X_i) \mod n, \\ f &\equiv (\sum \alpha''_i X_i)(\sum \beta''_i X_i) \mod m. \end{aligned}$$

Zu α_i', α_i'' gibt es ein α_i mit $\alpha_i \equiv \alpha_i' \mod n$ und $\alpha_i \equiv \alpha_i'' \mod m$, und entsprechend gibt es zu β_i', β_i'' ein β_i mit $\beta_i \equiv \beta_i' \mod n$ und $\beta_i \equiv \beta_i'' \mod m$ (die Surjektivitätsaussage des chinesischen Restsatzes). Also ist

$$f \equiv (\sum \alpha_i' X_i)(\sum \beta_i' X_i) \equiv (\sum \alpha_i X_i)(\sum \beta_i X_i) \mod n$$
$$f \equiv (\sum \alpha_i'' X_i)(\sum \beta_i'' X_i) \equiv (\sum \alpha_i X_i)(\sum \beta_i X_i) \mod m,$$

also auch

$$f \equiv (\sum \alpha_i X_i)(\sum \beta_i X_i) \mod nm$$

(die Injektivitätsaussage des chinesischen Restsatzes).

Zweimalige Anwendung des Lemmas zeigt nun, dass es ganze Zahlen α', β', γ', $\alpha'', \beta'', \gamma''$ gibt mit

$$(*) \qquad \alpha X^2 + \beta Y^2 + \gamma Z^2 \equiv \big(\alpha' X + \beta' Y + \gamma' Z\big)\big(\alpha'' X + \beta'' Y + \gamma'' Z\big) \mod \alpha\beta\gamma.$$

Beachte: Wegen $\alpha \neq 0$ sind auch $\alpha', \alpha'' \neq 0$, usw.

Wir brauchen ein zweites Lemma.

Lemma 2. *Seien λ, μ, ν positive reelle Zahlen, sei $n = \lambda\mu\nu \in \mathbb{N}$. Seien $\alpha, \beta, \gamma \in \mathbb{Z}$. Sei $f(x, y, z)$ eine Linearform mit Koeffizienten in $\mathbb{Z}$. Dann gibt es $[x, y, z] \neq 0$ in $\mathbb{Z}^3$ mit $f(x, y, z) \equiv 0 \mod n$ und $|x| \leq \lambda,\ |y| \leq \mu,,\ |z| \leq \nu$.*

Beweis: Wir beginnen, für x die Zahlen $0, 1, \ldots \lfloor\lambda\rfloor$ zu nehmen (dies sind $\lfloor\lambda\rfloor + 1$ Möglichkeiten). für y die Zahlen $0, 1, \ldots \lfloor\mu\rfloor$ (dies sind $\lfloor\mu\rfloor + 1$ Möglichkeiten). für z die Zahlen $0, 1, \ldots \lfloor\nu\rfloor$ (also $\lfloor\nu\rfloor + 1$ Möglichkeiten). Ingesamt betrachten wir also

$$(\lfloor\lambda\rfloor + 1)(\lfloor\mu\rfloor + 1)(\lfloor\mu\rfloor + 1) > \lambda\mu\nu = n$$

Tripel. Wir bilden die zugehörigen Werte $f(x, y, z)$ und deren Restklassen modulo n. Mindestens zwei dieser Restklassen müssen übereinstimmen: Es gibt also derartige Tripel $[x', y', z'] \neq [x'', y'', z'']$ mit

$$f(x', y', z') \equiv f(x'', y'', z'') \mod n,$$

wegen der Linearität ist also

$$f(x' - x'', y' - y'', z' - z'') \equiv 0 \mod n.$$

Wegen $[x', y', z'] \neq [x'', y'', z'']$ ist $[x' - x'', y' - y'', z' - z''] \neq 0$, wegen der Wahl von x', x'' ist $|x' - x''| \leq \lambda$, usw. Wir setzen also $x = x' - x'',\ y = y' - y'',\ z = z' - z''$.

Bevor wir fortfahren, wollen wir zwei Spezialfälle separat behandeln und die Vorzeichen geeignet wählen. Wir können annehmen, dass nur eine der drei Zahlen α, β, γ

positiv ist (sonst multiplizieren wir f mit -1) und dass dies α ist (sonst Vertauschung der Variablen).

Spezialfall 1: $\beta = \gamma = -1$. Dann ist $-1 = -\beta\gamma$ quadratischer Rest modulo α. Also wissen wir, dass sich α als Summe zweier Quadrate schreiben lässt, etwa $\alpha = y^2 + z^2$. Setzen wir $x = 1$, so sehen wir

$$\alpha x^2 + \beta y^2 + \gamma z^2 = \alpha \cdot 1^2 - 1 \cdot y^2 - 1 \cdot z^2 = 0.$$

Spezialfall 2: $\alpha = 1, \beta = -1$. In diesem Fall sind alle Tripel $[x, x, 0]$ Lösungen.

Wir nehmen nun an, dass keiner der beiden Spezialfälle vorliegt. Es gilt also

$$\beta\gamma > 1 \qquad \text{und} \qquad -\alpha\beta > 1.$$

Wir setzen

$$\lambda = \sqrt{\beta\gamma}, \quad \mu = \quad \sqrt{-\gamma\alpha}, \quad \nu = \quad \sqrt{-\alpha\beta}.$$

Da $\beta\gamma > 1$ und quadratfrei ist, sehen wir, dass λ keine ganze Zahl sein kann. Entsprechd folgt aus $-\alpha\beta >$ und der Tatsache, dass dies eine quadratfreie Zahl ist, dass auch ν nicht ganzzahlig ist.

Wir wenden Lemma 2 auf die Linearform $f(x, y, z) = \alpha' x + \beta' y + \gamma' z$ und die soeben definierten positiven reelen Zahlen λ, μ, ν an. Wir erhalten $x, y, z \in \mathbb{Z}$ mit $|x| \leq \lambda, |y| \leq \mu, |z| \leq \nu$ und $\alpha' x + \beta' y + \gamma' z \equiv 0 \mod \alpha\beta\gamma$. Wegen $(*)$ ist auch

$$\alpha x^2 + \beta y^2 + \gamma z^2 \equiv 0 \mod \alpha\beta\gamma$$

Da weder λ noch ν ganze Zahlen sind, folgt aus $|x| \leq \lambda$ und $|z| \leq \nu$, dass gilt:

$$|x| < \lambda \qquad \text{und} \qquad |z| < \nu.$$

Wir schauen uns $\alpha x^2 + \beta y^2 + \gamma z^2$ genauer an. Einerseits ist

$$\alpha x^2 + \beta y^2 + \gamma z^2 \leq \alpha x^2 < \alpha\lambda^2 = \alpha\beta\gamma$$

(die erste Ungleichung gilt, da β, γ beide negativ sind). Andererseits ist

$$\alpha x^2 + \beta y^2 + \gamma z^2 \geq \beta y^2 + \gamma z^2 > -2\alpha\beta\gamma$$

(die erste Ungleichung gilt, da α positiv ist, weiter verwenden wir, dass $\beta y^2 \geq \beta\mu^2 = -\alpha\beta\gamma$ gilt, und dass $z^2 > -\alpha\beta$ gilt: Wegen $\gamma > 0$, ist $\gamma z^2 > -\alpha\beta\gamma$). Insgesamt sehen wir:

$$-2\alpha\beta\gamma < \alpha x^2 + \beta y^2 + \gamma z^2 < \alpha\beta\gamma.$$

Da

$$\alpha x^2 + \beta y^2 + \gamma z^2 \equiv 0 \mod \alpha\beta\gamma,$$

folgt: Entweder ist

$$\alpha x^2 + \beta y^2 + \gamma z^2 = 0, \qquad \text{oder} \qquad \alpha x^2 + \beta y^2 + \gamma z^2 = -\alpha\beta\gamma.$$

Im ersten Fall ist $[x, y, z]$ eine gesuchte Lösung. Im zweiten Fall setzen wir

$$x_1 = -\beta y + xz, \quad y_1 = \alpha x + yz, \quad z_1 = z^2 + \alpha\beta.$$

Es ist

$$\begin{aligned}
\alpha x_1^2 + \beta y_1^2 + \gamma z_1^2 &= \alpha\big(-\beta y + xz\big)^2 + \beta\big(\alpha x + yz\big)^2 + \gamma\big(z^2 + \alpha\beta\big)^2 \\
&= \alpha\beta^2 y^2 - 2\alpha\beta xz + \alpha x^2 z^2 \\
&\quad + \beta\alpha^2 x^2 + 2\beta\alpha xyz + \beta y^2 z^2 \\
&\quad + \gamma z^4 + \gamma z^2\alpha\beta + \gamma z^2\alpha\beta + \gamma\alpha^2\beta^2 \\
&= \alpha\beta\big(\alpha x^2 + \beta y^2 + \gamma z^2 - \alpha\beta\gamma\big) \\
&\quad + \big(\alpha x^2 + \beta y^2 + \gamma z^2 - \alpha\beta\gamma\big) z^2 = 0
\end{aligned}$$

Beachte, dass $z_1 \neq 0$ gilt, dennn sonst wäre $z^2 = -\alpha\beta$. Aber $\alpha\beta$ ist quadratfrei, und demnach $z^2 = 1$ und $\alpha = 1,\ \beta = -1$; dies haben wir aber ausgeschlossen. Insgesamt sehen wir, dass im zweiten Fall $[x_1, y_1, z_1]$ eine gesuchte Lösung ist.

Der Spezialfall $x^2 + y^2 = \gamma z^2$ mit γ quadratfrei (und γ positiv). Wann gibt es eine nicht-triviale Lösung? Der Satz besagt: genau dann, wenn -1 eine Quadratzahl modulo γ ist. Aber das wissen wir ja. Ist γ quadratfrei, negativ und -1 Quadratzahl modulo γ, so liefert 5.4.1 eine nicht-triviale Lösung. Wir wissen aber schon, dass es dann zu jedem $z \neq 0$ eine Lösung gibt, insbesondere zu $z = 1$.