Wolfgang K. Seiler
Tel. 2515

B6, B4.18

25. Mai 2020

11. Übungsblatt Elliptische Kurven

Aufgabe 1: *(6 Punkte)*

Bestimmen Sie für jede der folgenden Zahlen n alle endlichen abelschen Gruppen der Ordnung n und schreiben Sie diese jeweils als Produkt möglichst weniger zyklischer Gruppen!

a) $n = 12$ *b)* $n = 30$ *c)* $n = 64$

Lösung:

a) $12 = 2^2 \cdot 3$; somit ist jede abelsche Gruppe der Ordnung zwölf das Produkt einer Gruppe der Ordnung vier und einer der Ordnung drei. Die einzige Gruppe der Ordnung drei ist $\mathbb{Z}/3$; Ordnung vier hat außer der zyklischen Gruppe $\mathbb{Z}/4$ noch $\mathbb{Z}/2 \times \mathbb{Z}/2$, die sogenannte Kleinsche Vierergruppe. Es gibt daher die beiden Gruppen

$$\mathbb{Z}/4 \times \mathbb{Z}/3 \cong \mathbb{Z}/12 \quad \text{und} \quad \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \cong \mathbb{Z}/6 \times \mathbb{Z}/2\,.$$

b) $30 = 2 \cdot 3 \cdot 5$ ist ein Produkt dreier Primzahlen. Zu jedem der drei Faktoren gibt es nur die zyklische Gruppe der entsprechenden Ordnung; daher ist $\mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/5 \cong \mathbb{Z}/30$ die einzige abelsche Gruppe der Ordnung dreißig.

c) $64 = 2^6$; somit ist jede abelsche Gruppe der Ordnung 64 Produkt von Gruppen der Ordnung 2^i, wobei die Summe der Exponenten sechs sein muß. Dies führt auf die Gruppen

$$\begin{gathered}
\mathbb{Z}/64, \quad \mathbb{Z}/32 \times \mathbb{Z}/2, \quad \mathbb{Z}/16 \times \mathbb{Z}/4, \quad \mathbb{Z}/8 \times \mathbb{Z}/8, \\
\mathbb{Z}/16 \times \mathbb{Z}/2 \times \mathbb{Z}/2, \quad \mathbb{Z}/8 \times \mathbb{Z}/4 \times \mathbb{Z}/2, \quad \mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}/4, \\
\mathbb{Z}/8 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2, \quad \mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2, \\
\mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2, \quad \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2
\end{gathered}$$

Aufgabe 2: *(8 Punkte)*

a) Zeigen Sie, daß eine abelsche Gruppe der Ordnung n zu jedem Teiler m von n mindestens eine Untergruppe der Ordnung m hat!

Lösung: Für eine zyklische Gruppe ist das klar: Wird die Gruppe erzeugt von einem Element P, so erzeugt für jeden Teiler $m|n$ das Element $\frac{n}{m}P$ eine Untergruppe der Ordnung m.

Eine beliebige abelsche Gruppe der Ordnung n läßt sich nach dem Struktursatz schreiben als ein Produkt $\mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$, wobei das Produkt der n_i gleich n ist. Zu jedem Teiler $m|n$ gibt es Teiler $m_i|n_i$ mit Produkt m, und jede der Gruppen $\mathbb{Z}/n_i$ hat eine Untergruppe G_i der Ordnung m_i. Das Produkt der G_i ist dann eine Untergruppe der Ordnung m.

b) Finden Sie ein Beispiel, bei dem es mehrere solche Untergruppen gibt!

Lösung: In $\mathbb{Z}/4 \times \mathbb{Z}/4$ sind $\mathbb{Z}/4 \times \{0\}$ und $\mathbb{Z}/2 \times \mathbb{Z}/2$ Untergruppen der Ordnung vier. Die eine ist zyklisch, die andere nicht.

c) Zeigen Sie, daß eine zyklische Gruppe der Ordnung n zu jedem Teiler m von n *genau* eine Untergruppe der Ordnung m hat!

Lösung: Die Gruppe sei erzeugt von P. Wir wollen uns zunächst überlegen, daß auch jede ihrer Untergruppen zyklisch ist: Die Untergruppe sei erzeugt von den Elementen $n_1P, \ldots, n_rP$. Da sich der ggT g der Koeffizienten $n_1, \ldots, n_r$ nach dem erweiterten Euklidischen Algorithmus als Linearkombination $g = a_1n_1 + \cdots + a_rn_r$ schreiben läßt, liegt auch

$$gP = a_1(n_1P) + \cdots + a_r(n_rP)$$

in der Untergruppe, und da jedes der Erzeugenden ein Vielfaches von gP ist, muß die Untergruppe gleich der von gP erzeugten zyklischen Gruppe sein.
Zu einer Untergruppe der Ordnung m können wir daher eine natürliche Zahl a finden derart, daß sie von aP erzeugt wird. Zu a und m gibt es ganze Zahlen c und d derart, daß $g = \mathrm{ggT}(a, m) = ca + dm$ ist. Da P die Ordnung m hat, liegt

$$gP = c(aP) + d(mP) = c(aP)$$

in der Untergruppe, und da g ein Teiler von a ist, erzeugt auch gP die gesamte Untergruppe. Jede Untergruppe der Ordnung m kann also auch erzeugt werden von einem Element gP, wobei g ein Teiler von n ist. Die von gP erzeugte Untergruppe hat die Ordnung n/g; somit ist $g = n/m$ der einzige Teiler von n, für den gP eine Untergruppe der Ordnung m erzeugt.

d) Eine natürliche Zahl n heißt quadratfrei, wenn in ihrer Primzerlegung keine Primzahl in einer höheren als der ersten Potenz auftritt. Zeigen Sie, daß in diesem Fall alle abelschen Gruppen der Ordnung n zueinander isomorph sind!

Lösung: Ist $n = p_1 \cdots p_r$ das Produkt der paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$, so ist die Gruppe isomorph zu einem Produkt aus r Faktoren, deren Ordnung $p_1, \ldots, p_r$ sind. Da es zu einer Primzahlordnung nur die zyklische Gruppe gibt, ist also

$$G \cong \mathbb{Z}/p_1 \times \cdots \times \mathbb{Z}/p_r\,,$$

was nach dem chinesischen Restesatz auch isomorph ist zu $\mathbb{Z}/n$.

Aufgabe 3: *(2 Punkte)*
Γ sei das Gitter $\mathbb{Z} + \mathbb{Z}i$ der Gaussschen Zahlen. Finden Sie eine doppeltperiodische Funktion mit Periodengitter Γ, die genau in den Punkten $n + mi$ und $n + \frac{1}{3} + mi$ mit $n, m \in \mathbb{Z}$ unendlich wird!

Lösung: $\wp$ sei die Weierstrasssche $\wp$-Funktion zum Gitter Γ. Dann wird $\wp(z)$ genau in den Punkten von Γ, also den Punkten der Form $n + mi$ mit $n, m \in \mathbb{Z}$ unendlich. Die Funktion $\wp(z - \frac{1}{3})$ wird genau dann unendlich, wenn $z - \frac{1}{3}$ in Γ liegt, also für Punkte der Form $n + \frac{1}{3} + mi$ mit $n, m \in \mathbb{Z}$. Somit hat beispielsweise die Funktion $f(z) = \wp(z) + \wp(z - \frac{1}{3})$ die gewünschte Eigenschaft.

Aufgabe 4: *(4 Punkte)*
Man sagt, eine Funktion $f\colon \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ habe im Punkt $z_0 \in \mathbb{C}$ einen Pol n-ter Ordnung, wenn sie in einer Umgebung von z_0 eine Potenzreihendarstellung der Form

$$f(z) = H(f) + \sum_{k=0}^{\infty} a_k z^k \quad \text{mit} \quad H(f) = \frac{a_{-n}}{(z-z_0)^n} + \cdots + \frac{a_{-1}}{z-z_0} \quad \text{und} \quad a_{-n} \neq 0$$

hat; die Funktion $H(f)$ heißt der *Hauptteil* von f im Punkt z_0.

a) $f\colon \mathbb{C} \to \mathbb{C} \cup \{\infty$ sei eine doppeltperiodische Funktion zum Gitter Γ, deren Einschränkung auf $\mathbb{C} \setminus \Gamma$ eine komplex differenzierbare Funktion $\mathbb{C} \setminus \Gamma \to \mathbb{C}$ sei, und die im Nullpunkt den Hauptteil $1/z^2$ habe. Zeigen Sie, daß f bis auf eine additive Konstante gleich der WEIERSTRASSschen $\wp$-Funktion ist!

Lösung: Da auch die WEIERSTRASSsche $\wp$-Funktion den Hauptteil $1/z^2$ hat, läßt sich die Differenz $f(z) - \wp$ um jeden Punkt von $\mathbb{C}$ durch eine TAYLOR-Reihe darstellen, ist also analytisch und damit komplex differenzierbar. Als doppeltperiodische stetige Funktion ist sie beschränkt auf ganz $\mathbb{C}$, als nach LIOUVILLE konstant.

b) Was können Sie über f sagen, wenn der Hauptteil im Nullpunkt stattdessen gleich $1/z^n$ ist?

Lösung: Im Falle $n = 1$ ohne entsprechende Kenntnisse der Funktionentheorie nichts; sei also $n \geq 2$.
$\wp(z)$ ist die Summe aus $1/z^2$ und einer analytischen Funktion. Die r-te Ableitung von $1/z^2$ ist $(r+1)!(-1)^r/z^{r+2}$, die einer analytischen Funktion ist natürlich wieder analytisch. Der Hauptteil von $\wp^{(n-2)}(z)$ ist somit $(n-1)!(-1)^n/z^n$, und

$$\frac{(-1)^n}{(n-1)!}\wp^{(r)}$$

hat den Hauptteil $1/z^n$. Wie in *a)* folgt, daß f bis auf eine additive Konstante gleich dieser Funktion sein muß.

c) Finden Sie zwei doppeltperiodische Funktionen mit einem Pol dritter *bzw.* vierter Ordnung im Nullpunkt, die kein skalares Vielfaches der Funktion $\wp(z)$ oder einer ihrer Ableitungen sind!

Lösung: Da gibt es viele Möglichkeiten. Beispielsweise hat $\wp(z) + \wp'(z)$ einen Pol der Ordnung drei im Nullpunkt und $\wp(z)^2$ einen der Ordnung vier.