Prof. Dr. Peter Bürgisser
Paul Breiding
Jesko Hüttenhain

Technische Universität Berlin
Fakultät II, Institut für Mathematik
Sekretariat MA 3-2

Übungen zur Vorlesung Algebra 2

Sommersemester 2014

Aufgabenzettel 8

Aufgabe 1 (15 Punkte). Man beschreibe die Konstruktion mit Zirkel und Lineal für das regelmäßige 5-Eck.

Aufgabe 2 (10 Punkte). Es sei $f(X) := X^3 + pX + q \in \mathbb{Q}[X]$ ein kubisches Polynom. Der Fall, dass f drei paarweise verschiedene reelle Nullstellen besitzt, wird *casus irreducibilis* genannt. Nimm an, dass der *casus irreducibilis* vorliegt.

(1) Zeige, dass $D := \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 < 0$.

(2) Nimm an, dass $z = r \cdot \cos\alpha$ eine Lösung von $f(X) = 0$ ist. Bestimme dann die drei Lösungen von $f(X) = 0$ unter Verwendung des Additionstheorems $(\cos\alpha)^3 = \frac{\cos 3\alpha + 3\cos\alpha}{4}$.

Bemerkung: $D < 0$ impliziert, dass in den Cardanischen Formeln die reellen Lösungen von $f(X) = 0$ als Summe von nicht-reelle Zahlen ausgedrückt werden. Dieses Phänomen wurde bereits vor Einführung der komplexen Zahlen entdeckt. Zwar konnte man damals wie heute einfach 'algebraisch' weiterrechnen und erhielt die korrekten Lösungen, dennoch ließ sich der Umstand, dass reelle Lösungen aus negativen Wurzeln entstanden, nicht erklären. Es gab keinen Ausweg aus dieser Situation, sie war *irreduzibel*, daher der Name *casus irreducibilis*.

Aufgabe 3 (15 Punkte). Es sei R ein Körper. Eine Präordnung auf R ist eine Teilmenge $T \subseteq R$, welche

- $T + T \subseteq T$, $TT \subseteq T$,
- $T \cap (-T) = \{0\}$,
- $a^2 \in T$ für alle $a \in R$

erfüllt. Eine Ordung P auf R ist eine Präordnung auf R, welche $P \cup (-P) = R$ erfüllt. Sei nun $\Sigma R^2 := \left\{ \sum_{i=1}^{n} a_i^2 | n \in \mathbb{N}, a_1, \ldots, a_n \in R \right\}$. Der Körper R heißt *formal reell*, falls $-1 \notin \Sigma R^2$. Zeige, dass ein Körper R genau dann eine Ordnung besitzt, wenn er formal reell ist. Gehe dazu wie folgt vor:

(1) Sei T eine Präordnung auf R und $a \notin T$. Zeige, dass dann auch $T - aT$ eine Präordnung auf R ist.

Prof. Dr. Peter Bürgisser
Paul Breiding
Jesko Hüttenhain

Technische Universität Berlin
Fakultät II, Institut für Mathematik
Sekretariat MA 3-2

(2) Zeige, dass zu jeder Präordnung T auf R eine Ordnung auf P existiert, sodass $T \subseteq P$. Verwende dazu das Lemma von Zorn und Aufgabenteil (1).

(3) Folgere, dass R genau dann eine Anordnung hat, wenn $-1 \notin \Sigma R^2$.

Bemerkung Besitzt R eine Ordnung P, so definiert man $a \leq b :\Leftrightarrow b - a \in P$. Falls $R = \mathbb{R}$, so ist die übliche Ordnung $P = \{x | x \geq 0\}$.

Aufgabe 4 (10 Punkte).

(1) Es sei p eine ungerade Primzahl. Eine Zahl $z \in \mathbb{Z}$ heißt quadratischer Rest $\bmod p$, falls ein $y \in \mathbb{Z}$ existiert, so dass $y^2 \equiv x \bmod p$. Wir definieren das Legendresymbol

$$\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \{-1, 0, 1\},$$
$$x \mapsto \begin{cases} 1, & \text{falls } \mathrm{ggT}(x,p) = 1 \text{ und } x \text{ ist quadratischer Rest } \bmod p \\ -1, & \text{falls } \mathrm{ggT}(x,p) = 1 \text{ und } x \text{ ist kein quadratischer Rest } \bmod p \\ 0, & \text{falls } p \mid x \end{cases}$$

Zeige, dass
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

(2) Folgere: Ist $x^2 + y^2 = p$ eine ungerade Primzahl, so gilt $4 \mid p - 1$.