Wolfgang K. Seiler
Tel. 2515

A5, C201

13. Februar 2016

Modulklausur Algebra

• • Lassen Sie bitte die obere Hälfte der Seite mit dem Aufkleber frei! • •
• • • Schreiben Sie bitte auf jedes Blatt Ihren Namen! • • •
• • • Die Aufgaben müssen *nicht* in der angegebenen Reihenfolge • • •
• • • bearbeitet werden; konzentrieren sie sich zunächst • • •
• • • auf das, womit sie schnell Punkte holen können! • • •

Aufgabe 1: (*12 Punkte*)
Für zwei Elemente g, h einer Gruppe G bezeichnet man $[g, h] = ghg^{-1}h^{-1}$ als den *Kommutator* von g und h; die kleinste Untergruppe von G, die alle Kommutatoren von Elementen aus G enthält, heißt die *Kommutatorgruppe* $[G, G]$ von G. Zeigen Sie:

a) Zwei Elemente von G kommutieren genau dann, wenn ihr Kommutator das Neutralelement e von G ist.

b) Falls in einer Gruppe G für jedes $g \in G$ die Gleichung $g^2 = e$ gilt, ist G abelsch.

c) Nun sei G wieder eine beliebige Gruppe, und g, h, x seien drei Elemente von G. Dann ist $[g, h]^x = [g^x, h^x]$.

d) $[G, G]$ ist ein Normalteiler von G, und $G/[G, G]$ ist eine abelsche Gruppe.

e) $\mathfrak{S}_n$ sei die symmetrische Gruppe aller Permutationen von n Elementen, und $\mathfrak{A}_n$ sei die Untergruppe der geraden Permutationen. Zeigen Sie: Für $n \geq 5$ ist $[\mathfrak{A}_n, \mathfrak{A}_n] = \mathfrak{A}_n$!

f) Auch $[\mathfrak{S}_n, \mathfrak{S}_n] = \mathfrak{A}_n$.

Aufgabe 2: (*8 Punkte*)
Zeigen Sie:

a) Jede rationale Zahl $x \in \mathbb{Q} \setminus \{0\}$ läßt sich eindeutig darstellen in der Form

$$x = \pm \prod_{i=1}^{r} p_i^{e_i}$$

mit Primzahlen $p_1 < p_2 < \cdots < p_r$ und ganzen Zahlen $e_i \neq 0$.

b) Falls für eine rationale Zahl x eine der Potenzen x^n, $n \in \mathbb{N}$, ganzzahlig ist, liegt auch x in $\mathbb{Z}$.

c) $f = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$ sei ein Polynom vom Grad mindestens zwei mit ganzzahligen Koeffizienten. Dann kann die Ableitung f' von f in $\mathbb{Z}[X]$ kein Teiler von f sein.

d) Wenn f' in $\mathbb{Q}[X]$ ein Teiler von f ist, gibt es ein $a \in \mathbb{Z}$, so daß $f = (X - a)^d$ ist.

• • • **Bitte wenden!** • • •

Aufgabe 3: *(8 Punkte)*

a) Zu ihrem großen Leidwesen können die Mitglieder des Männergesangsvereins Altoettinger Brummbass von 1888 am Valentinstag nicht alleine losziehen, ohne den Familienfrieden zu gefährden. Jedes Mitglied bringt daher, falls vorhanden, seine Frau oder Freundin mit, und wenn das Paar Kinder hat, dürfen auch die kommen. Um zehn Uhr morgens brechen achtundvierzig Personen auf. Um halb elf Uhr erreichen sie einen Stand, der Erfrischungen und Blumen verkauft. Jeder Mann konsumiert dort Bier im Wert von dreizehn Euro. Wegen des Valentinstags schenkt er, falls er nicht alleine unterwegs ist, seiner Begleiterin einen Blumenstrauß für fünf Euro, und falls er Kinder dabei hat, spendiert er jedem ein Eis für zwei Euro. Insgesamt nimmt der Stand dabei dreihundert Euro ein. Was können Sie über die Anzahl der Männer, Frauen und Kinder sagen?

b) Nun erfahren Sie zusätzlich, daß für die Anzahl n der Männer das regelmäßige n-Eck mit Zirkel und Lineal konstruiert werden kann. Wissen Sie jetzt mit Sicherheit, wie viele Männer, Frauen und Kinder unterwegs waren?

Aufgabe 4: *(6 Punkte)*

a) Einer Ihrer Bekannten benutzt ein RSA-System mit Modul N und öffentlichem Exponenten e; der Ihnen unbekannte private Exponent ist d, und die Funktion, mit der Ihr bekannter eine Nachricht $x \in \mathbb{Z}/N$ unterschreibt, sei $U\colon \mathbb{Z}/N \to \mathbb{Z}/N$. Zeigen Sie, daß für $x, y \in \mathbb{Z}/N$ gilt: $U(xy) = U(x)U(y)$.

b) Sie möchten gerne, daß Ihr Bekannter, der Teil *a)* nicht kennt, eine für Sie vorteilhafte Nachricht $m \in \mathbb{Z}/N$ unterschreibt. Dazu ist er leider nicht bereit, aber um Ihnen zu zeigen, wie das System funktioniert, sagt er zu, Ihnen eine von Ihnen gewählte sinnlose Nachricht x zu unterschreiben. Sie wählen eine Zufallszahl $z \in (\mathbb{Z}/N)^\times$ und legen ihm die Nachricht $x = mz^e \bmod N$ zur Unterschrift vor. Wie können Sie $U(m)$ aus $U(x)$ berechnen, und welche Algorithmen benötigen Sie dazu?

Aufgabe 5: *(4 Punkte)*

a) Faktorisieren Sie das Polynom $f = 21X^3 - 21$ in $\mathbb{Q}[X]$ und in $\mathbb{Z}[X]$!

b) Faktorisieren Sie f in $K[X]$ mit $K = \mathbb{Q}(\sqrt{-3})$!

Aufgabe 6: *(12 Punkte)*

a) Geben Sie eine $\mathbb{Q}$-Vektorraumbasis von $K = \mathbb{Q}(\sqrt[4]{5})$ an, und bestimmen Sie $\mathrm{Aut}(K/\mathbb{Q})$!

b) Zeigen Sie, daß $L = \mathbb{Q}(\sqrt[4]{5}, i)$ der Zerfällungskörper des Polynoms $X^4 - 5$ über $\mathbb{Q}$ ist!

c) Geben Sie eine K-Vektorraumbasis und eine $\mathbb{Q}$-Vektorraumbasis von L an!

d) $\sigma\colon L \to L$ sei der Automorphismus von $L/\mathbb{Q}$, der $\sqrt[4]{5}$ auf $i\sqrt[4]{5}$ abbildet und i festläßt. Zeigen Sie, daß σ in $\mathrm{Aut}(L/\mathbb{Q})$ die Ordnung vier hat!

e) Zeigen Sie, daß auch die komplexe Konjugation τ ein Automorphismus von $L/\mathbb{Q}$ ist, und bestimmen Sie den Fixkörper der Menge $\{\sigma, \tau\}$! *(Fangen Sie am besten an mit der Invarianz unter τ.)* Folgern Sie, daß $\mathrm{Aut}(L/\mathbb{Q})$ von σ und τ erzeugt wird, d.h. es gibt keine echte Untergruppe von $\mathrm{Aut}(L/\mathbb{Q})$, die sowohl σ als auch τ enthält!

f) Was ist $\mathrm{Aut}(L/K)$?