WOLFGANG K. SEILER
Tel. 2515

B6,26, A4.18

12. Dezember 2017

Modulklausur Algebra

• • • 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: *(6 Punkte)*

Bestimmen Sie alle Lösungen (einschließlich Vielfachheiten) der folgenden Gleichungen:

a) $x^2 - 4x + 1 = 8i - 4ix$

b) $x^7 - 2x^6 - 4x^5 + 8x^4 + 3x^3 - 6x^2 = 0$

Aufgabe 2: *(12 Punkte)*

G sei eine Gruppe. Zeigen Sie:

a) Die Menge Aut G aller Automorphismen von G ist eine Gruppe.

b) Für jedes $a \in G$ ist die Abbildung

$$\varphi_a \colon \begin{cases} G \to G \\ g \mapsto aga^{-1} \end{cases}$$

ein Automorphismus von G.

c) Die Abbildung $\psi\colon G \to \operatorname{Aut} G$, die jedem $a \in G$ den Automorphismus φ_a zuordnet, ist ein Gruppenhomomorphismus.

d) Der Kern von ψ ist das Zentrum von G.

e) Die Abbildung $\omega\colon G \to G$, die jedem Element g sein Inverses zuordnet, ist genau dann ein Gruppenhomomorphismus, wenn G abelsch ist.

f) $G = \mathbb{Z}/2 \times \mathbb{Z}/2$ sei die KLEINsche Vierergruppe. Geben Sie Aut G explizit an!

Aufgabe 3: *(4 Punkte)*

Zeigen Sie:

a) Die additive Gruppe der reellen Zahlen ist isomorph zur multiplikativen Gruppe der positiven reellen Zahlen.

b) Die additive Gruppe der rationalen Zahlen ist nicht isomorph zur multiplikativen Gruppe der positiven rationalen Zahlen. (*Hinweis:* Betrachten Sie, unter der Annahme, es gäbe einen Isomorphismus $\varphi\colon \mathbb{Q} \to \mathbb{Q}_{>0}$, die Elemente $\varphi(x/2)$ für $x \in \mathbb{Q}$.)

Aufgabe 4: *(8 Punkte)*

Die Rhineckar School of Commerce nimmt jedes Jahr maximal 115 Studenten der Wirtschaftsmathematik auf. Alle Studenten, die das dritte Studienjahr erreichen, werden im Herbstsemester pflichtangemeldet für die Klausuren in Wirtschaftsalgebra und in Wirtschaftsgeometrie. In den Hörsälen werden sie so gesetzt, daß in jeder Reihe außer eventuell der hintersten die gleiche Anzahl von Studenten sitzen. Im Falle der Wirtschaftsalgebra gibt es vier Wiederholer aus höheren Studienjahren und sechs Pflichtangemeldete, die nicht erschienen sind; in den vorderen Reihen sitzen jeweils dreizehn Prüflinge, in der hinteren sitzen zehn. Bei der Wirtschaftsgeometrie gibt es fünf Wiederholer und acht nicht Erschienene; hier sitzen in den vorderen Reihen jeweils neun Personen, in der hinteren nur eine. Wie viele Studenten sind im dritten Studienjahr eingeschrieben?

Aufgabe 5: *(8 Punkte)*

a) Für eine r-Primzahlen-Variante von RSA könnte man als Modul N das Produkt von r paarweise verschiedenen großen Primzahlen $p_1, \dots, p_r$ nehmen und dazu einen Exponenten e wählen, der teilerfremd ist zu jeder der r Zahlen $p_i - 1$ für $i = 1, \dots, r$. Zeigen Sie: Ist $\lambda(N)$ das kgV der $p_i - 1$, so gibt es $d, k \in \mathbb{N}$ mit $ed - k\lambda(N) = 1$, und für alle $m \in \mathbb{Z}$ ist $\left(m^e\right)^d \equiv m \bmod N$.

b) Könnte man statt mit $\lambda(N)$ auch mit einem beliebigen gemeinsamen Vielfachen der $p_i - 1$ arbeiten?

c) Warum verwendet man in der Kryptographie nur die Version mit $r = 2$?

Aufgabe 6: *(10 Punkte)*

a) Zeigen Sie, daß für jede Einheit z im Ring $R = \mathbb{Z} \oplus \mathbb{Z}i$ der GAUSSschen Zahlen das Produkt $z\overline{z}$ mit der konjugiert komplexen Zahl eine Einheit in $\mathbb{Z}$ ist, und bestimmen Sie die Gruppe aller Einheiten in R!

b) In R ist $1 + i$ ein irreduzibles Element. (Das müssen Sie nicht beweisen.) Bestimmen Sie die dazu assoziierten Elemente und zeigen Sie, daß sich die Zwei als Produkt von $1 + i$ mit einem dieser Elemente darstellen läßt!

c) Was ist der Inhalt des Polynoms $f = 10X^4 - 160 \in \mathbb{Z}[X]$?

d) Zerlegen Sie $f = 10X^4 - 160$ jeweils in $\mathbb{Z}[X]$ und in $\mathbb{Q}[X]$ in seine irreduziblen Bestandteile! Wie viele gibt es jeweils?

e) Zerlegen Sie f entsprechend auch in $R[X]$ und in $K[X]$, wobei $K = \mathbb{Q} \oplus \mathbb{Q}i$ den Quotientenkörper von R bezeichnet! Wie viele irreduzible Faktoren gibt es hier jeweils?

Aufgabe 7: *(12 Punkte)*

a) $K/\mathbb{Q}$ sei eine Körpererweiterung, $f \in \mathbb{Q}[X]$ ein Polynom mit rationalen Koeffizienten, und $z \in K$ sei eine Nullstelle von f. Zeigen Sie: Für jeden Automorphismus $\varphi\colon K \to K$ ist auch $\varphi(z)$ eine Nullstelle von f!

b) Ist der Körper $K = \mathbb{Q}\left(\sqrt{3}, \sqrt{11}\right)$ GALOISsch über $\mathbb{Q}$?

c) Das Polynom $f \in \mathbb{Q}[X]$ habe in $\mathbb{R}$ die Nullstelle $\sqrt{3} + \sqrt{11}$. Zeigen Sie, daß dann jede der vier Zahlen $\pm\sqrt{3} \pm \sqrt{11}$ Nullstelle von f ist!

d) Finden Sie ein Polynom $g \in \mathbb{Q}[X]$ mit positivem Grad, das jedes Polynom $f \in \mathbb{Q}[X]$ mit Nullstelle $\sqrt{3} + \sqrt{11}$ teilt!

e) Zeigen Sie, daß $L = \mathbb{Q}\left(\sqrt{3} + \sqrt{11}\right)$ gleich K ist und außerdem der Zerfällungskörper von g!

f) Zeigen Sie, daß $L/\mathbb{Q}$ GALOISsch ist und bestimmen Sie die GALOIS-Gruppe von $L/\mathbb{Q}$ sowie alle Zwischenkörper k mit $\mathbb{Q} \subset k \subset L$!