Wolfgang K. Seiler
Tel. 2515

A5, C201

16. Dezember 2015

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 eine Gruppe G bezeichnet man $Z(G) \underset{\text{def}}{=} \{x \in G \mid gx = xg \ \ \forall g \in G\}$ als das *Zentrum* von G. Zeigen Sie:

a) $Z(G)$ ist eine Untergruppe von G.

b) Für jeden Automorphismus $\varphi\colon G \to G$ ist $\varphi\big(Z(G)\big) = Z(G)$.

c) $Z(G)$ ist die Menge aller $x \in G$, die unter der Konjugation $x \mapsto x^g = g^{-1}xg$ mit jedem Element $g \in G$ auf sich selbst abgebildet werden.

d) $Z(G)$ ist ein Normalteiler von G.

e) Für ein beliebiges $x \in G$ sei $C_x = \{x^g \mid g \in G\}$ die Menge aller Konjugierten von x und $\mathrm{Stab}(x) = \{g \in G \mid x^g = x\}$ der Stabilisator von x unter der Konjugation. Zeigen Sie, daß im Falle einer endlichen Gruppe G gilt: $|C_x| \cdot |\mathrm{Stab}(x)| = |G|$, wobei $|M|$ für jede endliche Menge M deren Elementanzahl bezeichnet!

f) Nun sei G eine Gruppe, für die $|G| = p^n \neq 1$ Potenz einer Primzahl ist. Folgern Sie aus *e)*, daß $|Z(G)| > 1$ ist!

Aufgabe 2: (*8 Punkte*)

Zu einer Konferenz haben sich zweihundert Mathematiker angemeldet, die allerdings nicht alle kommen. Die Begrüßung, zu der alle Teilnehmer erscheinen, findet in einem Saal statt, in dem in jeder Reihe acht Plätze sind. Bei seiner Ansprache sieht der Leiter der Konferenz, daß zwar hinten noch einige Reihen frei sind, daß aber alle der vorderen Reihen voll besetzt sind. Nach der Begrüßung gehen alle Teilnehmer mit Ausnahme des Tagungsleiters und seiner beiden Stellvertreter zum Abendessen in einen Speisesaal mit runden Tischen, an denen je sieben Personen Platz haben. Als die drei nach ihrer Besprechung ebenfalls in den Speisesaal kommen, sehen sie, daß es zwar noch freie Tische gibt, daß aber alle übrigen Tische voll besetzt sind. Am nächsten Morgen finden parallel die Sitzungen von fünf Sektionen statt; jeder Teilnehmer geht zu der, die ihn am meisten interessiert. Wie sich herausstellt, haben alle Sektionen gleich viele Teilnehmer. Wie viele Mathematiker nahmen an der Konferenz teil? *(Hinweis: Wenn Sie wissen, was der erste Tag über die Teilnehmerzahl aussagt, können Sie ziemlich schnell direkt sehen, wie viele Teilnehmer die Konferenz hatte.)*

• • • **Bitte wenden!** • • •

Aufgabe 3: (*8 Punkte*)

a) Bei einem RSA-System wird (entgegen der Empfehlungen der Bundesnetzagentur) der öffentliche Exponent $e = 3$ benutzt; der Modul sei $N = pq$ mit $p, q > 3$. Zeigen Sie: Dann ist $p \equiv q \equiv 2 \bmod 3$ und

$$d = \frac{1 + 2\varphi(N)}{3}$$

ist eine natürliche Zahl, die als privater Exponent benutzt werden kann.

b) Bei einem konkreten (Spielzeug-)System sei

$$N = 91000000830000001 = (13 \cdot 10^7 + 1)(7 \cdot 10^8 + 1)$$

(mit Primzahlen als Faktoren) und $e = 3$. Bestimmen Sie den privaten Exponenten d!

c) Der Besitzer dieses Schlüssels will die Nachricht 1234567890 unterschreiben. Welche Zahl muß er berechnen? (Sie sollen die Berechnung *nicht* für ihn ausführen, sondern nur angeben, welchen Ausdruck er berechnen muß.)

d) Die Berechnung der Unterschrift führe auf das Ergebnis $u \in \mathbb{N}$. Was muß seine Vertragspartnerin tun, um die Richtigkeit der Unterschrift zu überprüfen?

Aufgabe 4: (*10 Punkte*)

a) Zeigen Sie: Hat das kubische Polynom $f = X^3 + aX^2 + bX + c \in \mathbb{Z}[X]$ eine doppelte Nullstelle, so sind alle Nullstellen von f ganzzahlig.

b) Das Polynom $f = 10X^3 - 120X^2 + 450X - 540 \in \mathbb{Z}[X]$ hat eine doppelte Nullstelle. Bestimmen Sie diese!

c) Zerlegen Sie f in $\mathbb{Z}[X]$ in seine irreduziblen Faktoren!

d) Zerlegen Sie f in $\mathbb{Q}[X]$ in seine irreduziblen Faktoren!

e) Zerlegen Sie $g = 20X^2 - 20X + 5 \in \mathbb{Z}[X]$ in seine irreduziblen Faktoren!

Aufgabe 5: (*12 Punkte*)

a) Zeigen Sie, daß $\mathbb{Q}(\sqrt{21}, \sqrt{27})$, $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ und $\mathbb{Q}(\sqrt{7} - \sqrt{3})$ derselbe Teilkörper K von $\mathbb{C}$ sind!

b) Welchen Grad hat die Körpererweiterung $K/\mathbb{Q}$? Geben Sie eine möglichst einfache Basis von $K/\mathbb{Q}$ an!

c) Was ist $\mathrm{Aut}(K/\mathbb{Q})$?

d) Bestimmen Sie alle Körper L mit $\mathbb{Q} < L < K$!

e) Finden Sie ein irreduzibles Polynom f derart, daß $k \cong \mathbb{Q}[X]/(f)$ ist!

f) Zerlegen Sie f über dem Körper $\mathbb{Q}(\sqrt{7})$ in seine irreduziblen Faktoren!