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.

Lösung: Natürlich liegt das Neutralelement in Z(G), denn $g \cdot 1 = 1 \cdot g = g$.
Für $x, y \in Z(G)$ und $g \in G$ ist $g(xy) = (gx)y = (xg)y = x(gy) = x(yg) = (xy)g$, so daß auch xy im Zentrum liegt.
Schließlich folgt aus $gx = xg$, daß $x^{-1}g^{-1} = g^{-1}x^{-1}$ ist; da mit g auch g^{-1} die sämtlichen Elemente von G durchläuft, liegt also mit x auch x^{-1} in Z(G).

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

Lösung: Sei $x \in Z(G)$ und $g \in G$ beliebig. Da ein Automorphismus bijektiv ist, gibt es ein $h \in G$, so daß $\varphi(h) = g$ ist, und wegen $x \in Z(G)$ ist $hx = xh$. Damit ist auch

$$g\varphi(x) = \varphi(h)\varphi(x) = \varphi(hx) = \varphi(xh) = \varphi(x)\varphi(h) = \varphi(x)g\,,$$

d.h. $\varphi(x)$ liegt in Z(G) und damit ist $\varphi\big(Z(G)\big) \subseteq Z(G)$. Da mit φ auch φ^{-1} ein Automorphismus ist, muß auch $\varphi^{-1}\big(Z(G)\big) \subseteq Z(G)$ sein, also $Z(G) \subseteq \varphi\big(Z(G)\big)$. Somit 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.

Lösung: x liegt genau dann in Z(G), wenn $gx = xg$ ist für alle $g \in G$. Diese Gleichung ist äquivalent zu $x = g^{-1}xg = x^g$, d.h. x liegt genau dann in Z(G), wenn $x^g = x$ ist für alle $g \in G$.

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

Lösung: Nach *c)* läßt die Konjugation mit einem beliebigen Element das Zentrum sogar punktweise fest, also erst recht als ganzes.
Alternativ: Da die Konjugation mit einem Element $g \in G$ eine Automorphismus von G ist, folgt dies auch aus *b)*.

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!

Lösung: Die Gruppe G operiert durch Konjugation auf sich selbst via

$$\begin{cases} G \times G \to G \\ (g, x) \mapsto x^g \end{cases}$$

Die Bahn eines Elements x ist die Menge C_x aller seiner Konjugierten, der Stabilisator ist $\mathrm{Stab}(x)$. Somit ist die Behauptung äquivalent zur Bahnbilanzgleichung für diese Operation.

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!

Lösung: Wie in *e)* operiere G auf sich selbst durch Konjugation. Für die Elemente des Zentrums ist der Stabilisator nach *c)* gleich der ganzen Gruppe, die Bahn daher einelementig. Es gibt mindestens ein Element des Zentrums, nämlich das Neutralelement. Für jedes Gruppenelement, das nicht im Zentrum liegt, ist der Stabilisator eine echte Untergruppe von G, deren Ordnung nach LAGRANGE eine p-Potenz sein muß; nach der Bahnbilanzgleichung ist die Länge der Bahn daher eine von der Eins verschiedenen p-Potenz. G ist die disjunkte Vereinigung endlich vieler Bahnen; bestünde das Zentrum nur aus der Eins, hätte genau eine dieser Bahnen die Länge eins, alle anderen Längen wären echte p-Potenzen. Da die Summe aller Längen gleich der Gruppenordnung p^n sein muß, ist das nicht möglich; $Z(G)$ ist also eine Untergruppe, die nicht nur aus der Eins besteht.

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.)*

Lösung: Gesucht ist eine Zahl $0 < x < 200$, die den Bedingungen

$$x \equiv 1 \bmod 8, \qquad x \equiv 3 \bmod 7 \quad \text{und} \quad x \equiv 0 \bmod 5$$

genügt. Beginnen wir mit den ersten beiden Gleichungen. Da $8 - 7 = 1$ ist, folgt

$$8 \equiv \begin{cases} 0 \bmod 8 \\ 1 \bmod 7 \end{cases} \quad \text{und} \quad -7 \equiv \begin{cases} 1 \bmod 8 \\ 0 \bmod 7 \end{cases};$$

somit ist $-7+8\cdot 3 = 17$ eine Lösung der ersten beiden Kongruenzen. Da 7 und 8 teilerfremd sind und $7 \cdot 8 = 56$, sind die sämtlichen Lösungen in N die Zahlen $17 + 56r$ mit $r \in \mathbb{N}_0$. Modulo fünf ist $17 + 56r \equiv 2 + r$, also ist dies erstmalig für $r = 3$ durch fünf teilbar, und $x = 17 + 3 \cdot 56 = 185$ ist die kleinste Lösung. Da die Lösung modulo $5 \cdot 7 \cdot 8 = 280$ eindeutig ist, gibt es keine weitere Lösung zwischen Null und zweihundert; also nahmen 185 Mathematiker teil.

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.

Lösung: Da $e = 3$ teilerfremd zu $\varphi(N) = (p-1)(q-1)$ sein muß, kann weder $p-1$ noch $q-1$ durch drei teilbar sein. Auch p und q können als Primzahlen größer drei nicht durch drei teilbar sein. Damit bleibt für beide nur noch die Möglichkeit, daß sie Dreierrest zwei haben.
Dann ist $\varphi(N) = (p-1)(q-1) \equiv 2 \cdot 2 \equiv 1 \bmod 3$, also ist $1 + 2\varphi(N)$ durch drei teilbar und $d \in \mathbb{N}$.

$$ed = 3d = 1 + 2\varphi(N) \equiv 1 \bmod \varphi(N)\,,$$

und genau diese Bedingung stellt sicher, daß $(a^e)^d \equiv a \bmod N$ für alle $a \in \mathbb{Z}$.

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!

Lösung: $\varphi(N) = (p-1)(q-1) = 13 \cdot 10^7 \cdot 7 \cdot 10^8 = 91 \cdot 10^{15}$, und nach *a)* können wir

$$d = \frac{1 + 2\varphi(N)}{3} = \frac{182 \cdot 10^{15} + 1}{3}$$

als privaten Exponenten nehmen.

$$\begin{aligned} &182\,000\,000\,000\,000\,001 : 3 \\ =\ &60\,666\,666\,666\,666\,667\,, \end{aligned}$$

also ist $d = 60\,666\,666\,666\,666\,667$.

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.)

Lösung: Er muß $u = 1234567890^d \bmod N$ berechnen.

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?

Lösung: Sie überprüft, ob $u^3 \equiv 1234567890 \bmod N$ ist.

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.

Lösung: Die doppelte Nullstelle ist einfache Nullstelle der Ableitung f'; da ein kubisches Polynom nicht mehr als eine doppelte Nullstelle haben kann, ist der ggT von f und f' somit ein lineares Polynom. Wegen der Faktorialität von $\mathbb{Z}[X]$ liegt es in $\mathbb{Z}[X]$, und als Teiler von f muß es höchsten Koeffizienten eins (oder -1) haben. Daher ist seine Nullstelle eine ganze Zahl z. Da z eine doppelte Nullstelle von f ist, ist f in $\mathbb{Z}[X]$ durch $(X-z)^2 = X^2 - 2zX + z^2$ teilbar, und der Quotient hat höchsten Koeffizienten eins. Also ist auch seine Nullstelle ganz.

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

Lösung: Wir können uns auf seinen primitiven Anteil $f^* = X^3 - 12X^2 + 45X - 54$ beschränken; der hat die Ableitung $3X^2 - 24X + 45$. Die doppelte Nullstelle von f ist Nullstelle davon, also auch von $X^2 - 8X + 15$. Die beiden Lösungen dieser quadratischen Gleichung haben Summe acht und Produkt fünfzehn, sind also drei und fünf. Da

$$f^*(3) = 27 - 12 \cdot 9 + 45 \cdot 3 - 54 = 27 \cdot (1 - 4 + 5 - 2) = 0$$

verschwindet, ist $z = 3$ die doppelte Nullstelle.

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

Lösung: Die Summe aller drei Nullstellen von f^* ist nach VIÈTE gleich 12; da drei eine doppelte Nullstelle ist, muß die noch fehlende Nullstelle sechs sein, d.h. $f^* = (X-3)^2(X-6)$. Damit ist $f = 2 \cdot 5 \cdot (X-3)^2 \cdot (X-6)$ die Zerlegung von f in $\mathbb{Z}[X]$.

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

Lösung: In $\mathbb{Q}[X]$ sind zwei und fünf keine irreduziblen Elemente mehr, sondern Einheiten. Daher ist dort $f = 10 \cdot (X-3)^2(X-6) = (X-3)^2 \cdot (10X - 60)$.

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

Lösung: $g = 5 \cdot (4X^2 - 4X + 1) = 5 \cdot \big((2X)^2 - 2 \cdot (2X) + 1\big) = 5 \cdot \big((2X) - 1\big)^2 = 5 \cdot (2X-1)^2$

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!

Lösung: Da $\sqrt{21} = \sqrt{3} \cdot \sqrt{7}$ und $\sqrt{27} = 3\sqrt{3}$, liegen $\sqrt{21}$ und $\sqrt{27}$ in $\mathbb{Q}(\sqrt{3}, \sqrt{7})$; genauso liegt auch $\sqrt{3} = \frac{1}{3}\sqrt{27}$ in $\mathbb{Q}(\sqrt{21}, \sqrt{27})$, und damit auch der Quotient $\sqrt{21}/\sqrt{3} = \sqrt{7}$. Somit ist $\mathbb{Q}(\sqrt{3}, \sqrt{7}) = \mathbb{Q}(\sqrt{21}, \sqrt{27})$.
$k = \mathbb{Q}(\sqrt{7} - \sqrt{3})$ liegt natürlich in $\mathbb{Q}(\sqrt{3}, \sqrt{7})$. Als Körper enthält k auch das Quadrat $(\sqrt{7} - \sqrt{3})^2 = 10 - 2\sqrt{21}$, also auch $\sqrt{21}$ und $\sqrt{21}(\sqrt{7} - \sqrt{3}) = (7\sqrt{3} - 3\sqrt{7})$. Damit liegt auch $(7\sqrt{3} - 3\sqrt{7}) + 3(\sqrt{7} - \sqrt{3}) = 4\sqrt{3}$ in k, also auch $\sqrt{3}$ und $\sqrt{7} = \sqrt{21}/\sqrt{3}$. Also ist $k = \mathbb{Q}(\sqrt{3}, \sqrt{7})$.

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

Lösung: $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$ enthält den Körper $\mathbb{Q}(\sqrt{3})$; als Vektorraum über $\mathbb{Q}(\sqrt{3})$ ist $K = \mathbb{Q}(\sqrt{3}) \oplus \mathbb{Q}(\sqrt{3})\sqrt{7}$. Da $\mathbb{Q}(\sqrt{3}) = \mathbb{Q} \oplus \mathbb{Q}\sqrt{3}$ ist, folgt $K = \mathbb{Q} \oplus \mathbb{Q}\sqrt{3} \oplus \mathbb{Q}\sqrt{7} \oplus \mathbb{Q}\sqrt{21}$. Damit ist $[K : \mathbb{Q}] = 4$.

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

Lösung: Ein Automorphismus $\varphi \in \mathrm{Aut}(K/\mathbb{Q})$ muß $\mathbb{Q}$ festlassen, ist also eindeutig bestimmt durch die Bilder der Basiselemente. Natürlich muß $\varphi(1) = 1$ sein. Da $\big(\sqrt{3}\big)^2 = 3$ ist, muß auch $\varphi(\sqrt{3})^2 = \varphi(3) = 3$ sein, d.h. $\varphi(\sqrt{3}) = \pm\sqrt{3}$. Ein analoges Argument zeigt, daß $\varphi(\sqrt{7}) = \pm\sqrt{7}$ sein muß. Das noch fehlende Bild $\varphi(\sqrt{21}) = \varphi(\sqrt{3}) \cdot \varphi(\sqrt{7})$ ist durch die Bilder von $\sqrt{3}$ und $\sqrt{7}$ festgelegt. Also haben wir vier Automorphismen; abgesehen von der Identität sind dies die Abbildungen ρ, σ, τ mit $\rho(\sqrt{3}) = -\sqrt{3}$ und $\rho(\sqrt{7}) = \sqrt{7}$, $\sigma(\sqrt{3}) = \sqrt{3}$ und $\sigma(\sqrt{7}) = -\sqrt{7}$, $\tau(\sqrt{3}) = -\sqrt{3}$ und $\tau(\sqrt{7}) = -\sqrt{7}$.

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

Lösung: Die Erweiterung $K/\mathbb{Q}$ ist GALOISsch, denn ist $x = a + b\sqrt{3} + c\sqrt{7} + d\sqrt{21}$ ein Element des Fixkörpers von $\mathrm{Aut}(K/\mathbb{Q})$, ist $\rho(x) = a - b\sqrt{3} + c\sqrt{7} - d\sqrt{21} = x$, also ist wegen der Eindeutigkeit der Basisdarstellung $b = d = 0$. Genauso folgt aus $\sigma(x) = x$, daß $c = 0$ sein muß. Daher ist $x = a \in \mathbb{Q}$, der Fixkörper ist also $\mathbb{Q}$.

Die GALOIS-Gruppe hat vier Elemente; außer der Identität erzeugt jedes eine Untergruppe der Ordnung zwei. Die Zwischenkörper sind daher

$$K^{<\rho>} = \mathbb{Q}(\sqrt{7}), \qquad K^{<\sigma>} = \mathbb{Q}(\sqrt{3}) \quad \text{und} \quad K^{<\tau>} = \mathbb{Q}(\sqrt{21}),$$

wobei $< g >$ jeweils die von einem Element g erzeugte zyklische Untergruppe bezeichnet.

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

Lösung: Wir wissen aus *a)*, daß $(\sqrt{7} - \sqrt{3})^2 = 10 - 2\sqrt{21}$ ist. Für $x = \sqrt{7} - \sqrt{3}$ ist also $(x^2 - 10)^2 = 4 \cdot 21 = 84$, d.h. $f = X^4 - 20X^2 + 16$ hat $\sqrt{7} - \sqrt{3}$ als Nullstelle. Da $\mathbb{Q}(x)/\mathbb{Q}$ eine Erweiterung vom Grad vier ist, folgt $K \cong \mathbb{Q}[X]/(f)$.

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

Lösung: Wegen $(\sqrt{7} + \sqrt{3})^2 = 10 + 2\sqrt{21}$ ist auch $y = \sqrt{7} + \sqrt{3}$ eine Nullstelle von f; da in f nur gerade Potenzen vorkommen, sind außerdem noch $-x$ und $-y$ Nullstellen. In K hat f daher die Nullstellen $\pm 3 \pm 7$, das heißt

$$\begin{aligned} f &= (X + \sqrt{3} + \sqrt{7})(X - \sqrt{3} + \sqrt{7})(X + \sqrt{3} - \sqrt{7})(X - \sqrt{3} - \sqrt{7}) \\ &= \big((X + \sqrt{7})^2 - 3\big)\big((X - \sqrt{7})^2 - 3\big) \\ &= (X^2 + 2\sqrt{7}X + 4)(X^2 - 2\sqrt{7}X + 4)\,. \end{aligned}$$

Die beiden Faktoren $X^2 \pm 2\sqrt{7}X + 4$ liegen in $\mathbb{Q}(\sqrt{7})[X]$ und sind dort irreduzibel, denn ein reduzibles quadratisches Polynom müßte eine Nullstelle in $\mathbb{Q}(\sqrt{7})$ haben, aber keine der Nullstellen $\pm\sqrt{7} \pm \sqrt{3}$ von f liegt in $\mathbb{Q}(\sqrt{7})$.