Wolfgang K. Seiler
Tel. 2515

B6,26, A4.18

12. Dezember 2017

Modulklausur Algebra

Aufgabe 1: (*6 Punkte*)

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

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

Lösung: Bringt man alle mit x behafteten Terme auf die linke Seite und den Rest auf die rechte, wir die Gleichung zu $x^2 - (4-4i)x = -1 + 8i$ (d.h. $p = -4 + 4i$ und $q = 1 - 8i$) oder $\big(x - (2-2i)\big)^2 - (2-2i)^2 = -1 + 8i$.

$(2-2i)^2 = -8i$, also wir die Gleichung zu $\big(x - (2-2i)\big)^2 = -1$, d.h. $x = 2 - 2i \pm i$. Die beiden Lösungen sind somit $2 - i$ und $2 - 3i$, und beides sind einfache Nullstellen.

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

Lösung: Da man x^2 ausklammern kann, ist $x = 0$ eine doppelte Nullstelle; die restlichen Nullstellen sind die des Polynoms $f = x^5 - 2x^4 - 4x^3 + 8x^2 + 3x - 6$. Das Produkt dieser Nullstellen ist nach Viète gleich sechs; es lohnt sich daher, die Teiler von sechs durchzuprobieren: $f(1) = 0$, $f(-1) = 0$ und $f(2) = 0$. Das Produkt dieser drei Nullstellen ist -2; das Produkt der restlichen beiden muß also gleich -3 sein. $f(3) = 48$ und $f(-3) = -240$, somit sind sie nicht ganzzahlig. Die Summe aller Nullstellen ist zwei, die der drei gefundenen auch, also haben die beiden fehlenden die Summe Null, sind also entgegengesetzt gleich und damit $\pm\sqrt{3}$. Da f den Grad fünf und fünf verschiedene Nullstellen hat, sind alle Nullstellen von f einfach. Die Ausgangsgleichung hat somit die Lösungen $x = 0$ mit Vielfachheit zwei sowie die Lösungen $1, -1, 2, \sqrt{3}$ und $-\sqrt{3}$ jeweils mit Vielfachheit eins.

Aufgabe 2: (*12 Punkte*)

G sei eine Gruppe. Zeigen Sie:

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

Lösung: Gruppenoperation ist die Hintereinanderausführung, und die Hintereinanderausführung zweier Automorphismen ist natürlich wieder ein Automorphismus. Neutralelement ist die identische Abbildung, invers ist jeweils die Umkehrabbildung, und die Verknüpfung von Abbildungen ist immer assoziativ.

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.

Lösung: Für zwei Elemente $g, h \in G$ ist

$$\varphi_a(gh) = agha^{-1} = ag(a^{-1}a)ha^{-1} = (aga^{-1})(aha^{-1}) = \varphi_a(g)\varphi_a(h)\,.$$

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

Lösung: Für $a, b \in G$ ist $\psi(ab) = \varphi_{ab}$, und für alle $g \in G$ ist

$$\varphi_{ab}(g) = abg(ab)^{-1} = abgb^{-1}a^{-1} = \varphi_a\big(\varphi_b(g)\big) = (\varphi_a \circ \varphi_b)(g)\,,$$

d.h. $\psi(ab) = \psi(a) \circ \psi(b)$.

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

Lösung: Liegt $a \in G$ im Kern von ψ, so ist φ_a die identische Abbildung, d.h. $aga^{-1} = g$ für alle $g \in G$. Multipliziert man beide Seiten von rechts mit a, folgt $ag = ga$, das Element a kommutiert also mit jedem Gruppenelement und liegt somit im Zentrum. Umgekehrt ist für ein a aus dem Zentrum $\varphi_a(g) = aga^{-1} = gaa^{-1} = g$ für alle $g \in G$, d.h. φ_a ist die identische Abbildung, so daß a im Kern von ψ liegt.

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

Lösung: Die Inversenbildung ist genau dann ein Gruppenhomomorphismus, wenn für alle $g, h \in G$ gilt $(gh)^{-1} = g^{-1}h^{-1}$. In jeder Gruppe ist $(gh)^{-1} = h^{-1}g^{-1}$; also ist dies äquivalent zu $g^{-1}h^{-1} = h^{-1}g^{-1}$ und damit auch $gh = hg$ für alle $g, h \in G$.

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

Lösung: G enthält die Identität e, zwei Elemente g, h mit $g^2 = h^2 = e$ und $gh = hg$, sowie dieses Element gh, für das $(gh)^2 = ghgh = ghhg = gg = e$ ebenfalls gleich dem Neutralelement ist. Außerdem ist $g(gh) = h$ und $h(gh) = h(hg) = g$, d.h. die drei Elemente g, h und gh haben alle die Ordnung zwei und das Produkt von je zweien von ihnen ist das dritte. Ein Automorphismus kann diese drei Elemente daher beliebig permutieren; die Automorphismengruppe ist also die volle Permutationsgruppe $\mathfrak{S}_3$ auf der Menge dieser drei Elemente. Schreibt man die vier Elemente als $(0,0)$, $(0,1)$, $(1,0)$ und $(1,1)$ bleibt also $(0,0)$ als Neutralelement fest, und die anderen drei werden durch $\mathfrak{S}_3$ permutiert.

Aufgabe 3: *(4 Punkte)*

Zeigen Sie:

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

Lösung: Die Exponentialfunktion bildet $\mathbb{R}$ bijektiv ab auf $\mathbb{R}_{>0}$, und nach ihrer Funktionalgleichung ist $e^{x+y} = e^x \cdot e^y$ für alle $x, y \in \mathbb{R}$.

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 $x \in \mathbb{Q}$.)

Lösung: Angenommen, $\varphi\colon \mathbb{Q} \to \mathbb{Q}_{>0}$ wäre ein Isomorphismus. Für jedes $x \in \mathbb{Q}$ wäre dann $\varphi(x/2) \cdot \varphi(x/2) = \varphi(x/2 + x/2) = \varphi(x)$; wegen der Surjektivität von φ wäre also jede positive rationale Zahl Quadrat einer anderen positiven rationalen Zahl. Da beispielsweise $\sqrt{2} \notin \mathbb{Q}$, ist das ein Widerspruch.

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?

Lösung: x sei die gesuchte Anzahl der Studenten im dritten Studienjahr. Dann sind, zusammen mit den Wiederholern, $x+4$ Studenten zur Wirtschaftsalgebra und $x+5$ zur Wirtschaftsgeometrie angemeldet. Sechs *bzw.* acht davon erscheinen nicht; im Hörsaal sind also $x-2$ *bzw.* $x-3$ Studenten. Somit ist $x-2 \equiv 10 \bmod 13$ und $x-3 \equiv 1 \bmod 9$, also

$$x \equiv 12 \bmod 13 \quad \text{und} \quad x \equiv 4 \bmod 9\,.$$

Da dreizehn und neun teilerfremd sind, kann aus diesen beiden Kongruenzen die Restklasse von x modulo $13 \cdot 9 = 117$ bestimmt werden:

$$\begin{aligned} 13 : 7 = 1 \text{ Rest } 4 &\Longrightarrow 4 = 1 \cdot 13 - 1 \cdot 9 \\ 9 : 4 = 2 \text{ Rest } 1 &\Longrightarrow 1 = 9 - 2 \cdot (13 - 9) = 3 \cdot 9 - 2 \cdot 13\,. \end{aligned}$$

Somit ist

$$-2 \cdot 13 = -26 \equiv \begin{cases} 0 & \bmod 13 \\ 1 & \bmod 9 \end{cases} \quad \text{und} \quad 3 \cdot 9 = 27 \equiv \begin{cases} 1 & \bmod 13 \\ 0 & \bmod 9 \end{cases},$$

und $27 \cdot 12 - 26 \cdot 4 = 220 \equiv \begin{cases} 12 & \bmod 13 \\ 4 & \bmod 9 \end{cases}$, genauso auch jedes $x \equiv 220 \bmod 117$.
Da $0 \le x \le 115$, muß $x = 103$ sein; im dritten Studienjahr sind also 103 Studenten 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 $p_1, \ldots, p_r$ nehmen und dazu einen Exponenten e wählen, der teilerfremd ist zu jeder der r Zahlen $p_i - 1$ für $i = 1, \ldots, r$. 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 $\left(m^e\right)^d \equiv m \bmod N$.

Lösung: Da e teilerfremd zu allen $p_i - 1$ gewählt wurde, ist e auch teilerfremd zum kgV $\lambda(N)$; mit dem erweiterten EUKLIDischen Algorithmus lassen sich daher $d, k \in \mathbb{Z}$ finden, so daß $de - k\lambda(N)$ gleich dem ggT eins ist. Falls d negativ sein sollte, kann man durch Addition eines Vielfachen der Gleichung $\lambda(N)e - e\lambda(N) = 0$ erreichen, daß es positiv wird; dann muß k automatisch ebenfalls positiv sein.
Für jede der Primzahlen p_i ist $k\lambda(N)$ ein Vielfaches von $p_i - 1$; für ein zu p_i teilerfremdes $m \in \mathbb{Z}$ ist daher $m^{k\lambda(N)} \equiv 1 \bmod p_i$ nach dem kleinen Satz von FERMAT und damit auch $m^{ed} = m^{1+k\lambda(N)} \equiv m \bmod p_i$. Diese Kongruenz gilt auch, wenn m nicht teilerfremd zu p_i ist, denn dann sind beide Seiten durch p_i teilbar, also kongruent Null modulo p_i. Da diese Kongruenz somit für alle $m \in \mathbb{Z}$ und für alle p_i gilt, gilt sie auch modulo dem Produkt N aller p_i.

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

Lösung: Nur, wenn dieses Vielfache λ teilerfremd zu e gewählt wird; denn andernfalls ist $\mathrm{ggT}(e, \lambda) > 1$, so daß man kein d mit $ed \equiv 1 \bmod \lambda$ finden kann.

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

Lösung: Bei gleicher Größenordnung von N müßten die Primzahlen p_i für $r > 2$ deutlich kleiner gewählt werden als für $n = 2$. Kleinere Faktoren lassen sich aber zumindest tendeziell leichter finden als große, so daß das Verfahren unsicherer wird.

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!

Lösung: Die Einheiten sind die Elemente, die ein multiplikatives Inverses in R haben. Ist $zw = 1$, so ist auch $\overline{z}\,\overline{w} = \overline{zw} = 1$, also ist auch $\overline{z}$ eine Einheit und damit auch das Produkt $z\overline{z}$. Genau wie sein Inverses $w\overline{w}$ liegt es in $\mathbb{Z}$, ist also eine Einheit von $\mathbb{Z}$.
Für $z = a + bi$ ist $\overline{z} = a - bi$ und $z\overline{z} = a^2 + b^2$; für eine Einheit z in R muß das eine Einheit in $\mathbb{Z}$ sein, also ± 1, wobei -1 natürlich nicht in Frage kommt. Also ist $a^2 + b^2 = 1$, d.h. entweder $a = \pm 1$ und $b = 0$ oder $a = 0$ und $b = \pm 1$. Die Einheitengruppe ist somit $R^\times = \{1, -1, i, -i\}$.

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!

Lösung: Die Assoziierten eines Elements sind seine Produkte mit Einheiten, hier also

$$1 + i, \quad -1 - i, \quad i(1 + i) = -1 + i \quad \text{und} \quad -i(1 + i) = 1 - i\,.$$

Nach der dritten binomischen Formel ist $2 = (1 + i)(1 - i)$.

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

Lösung: Der Inhalt ist der ggT der Koeffizienten, hier also 10

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?

Lösung: In $\mathbb{Z}[X]$ ist $f = 10(X^4 - 16) = 2 \cdot 5 \cdot (X^2 + 4)(X^2 - 4) = 2 \cdot 5 \cdot (X^2 + 4)(X + 2)(X - 2)$, und alle fünf Faktoren sind irreduzibel, denn 2 und 5 sind Primzahlen, $X \pm 2$ ist linear, und $X^2 + 4$ ist quadratisch ohne ganzzahlige Nullstelle. Somit ist dies die Faktorisierung von f in $\mathbb{Z}[X]$.
In $\mathbb{Q}[X]$ sind die drei polynomialen Faktoren weiterhin irreduzibel, denn $X^2 + 4$ hat auch keine rationale Nullstellen (oder alternativ, weil alle drei Polynome primitiv sind und damit nach Gauss genau dann irreduzibel in $\mathbb{Q}[X]$, wenn sie irreduzibel in $\mathbb{Z}[X]$ sind). Der Faktor $10 = 2 \cdot 5$ ist aber in $\mathbb{Q}$ und in $\mathbb{Q}[X]$ eine Einheit, so daß es hier nur drei irreduzible Faktoren gibt.

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?

Lösung: In R ist $2 = (1+i)(1-i) = (-i)(1+i)^2$, und entsprechend ist auch $5 = (2+i)(2-i)$, wobei hier aber die beiden Zahlen $2 + i$ und $2 - i$ *nicht* assoziiert sind: Kein Produkt von $2 + i$ mit einer der vier Einheiten ist $2 - i$. In R[X] zerfällt $(X^2 + 4) = (X + 2i)(X - 2i)$ in Linearfaktoren; die vollständige Zerlegung von f in R[X] ist somit

$$\begin{aligned} f &= (1 + i)(1 - i)(2 + i)(2 - i)(X + 2i)(X - 2i)(X + 2)(X - 2) \\ &= (-i)(1 + i)^2(2 + i)(2 - i)(X + 2i)(X - 2i)(X + 2)(X - 2)\,, \end{aligned}$$

wobei in der ersten Darstellung alle Faktoren irreduzibel in R[X] sind, in der zweiten alle außer der Einheit $(-i)$. Die Anzahl irreduzibler Faktoren ist also acht. In K[X] sind alle Faktoren aus R Einheiten, die Faktorisierung ist also $f = 10(X + 2i)(X - 2i)(X + 2)(X - 2)$ mit vier irreduziblen Faktoren und der Einheit zehn.

Aufgabe 7: (*12 Punkte*)

a) K/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!

Lösung: Sei $f = a_d X^d + \cdots + a_1 X + a_0$ mit $a_i \in \mathbb{Q}$. Jeder Automorphismus von K ist auf $\mathbb{Q}$ die Identität; aus $f(z) = a_d z^d + \cdots + a_1 z + a_0 = 0$ folgt daher, daß auch

$$\varphi\big(f(z)\big) = \varphi(a_d)\varphi(z)^d + \cdots + \varphi(a_1)\varphi(z) + \varphi(a_0) = a_d\varphi(z)^d + \cdots + a_1\varphi(z) + a_0 = f\big(\varphi(z)\big)$$

verschwindet.

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

Lösung: Als $\mathbb{Q}$-Vektorraum hat K z.B. die Basis $1, \sqrt{3}, \sqrt{11}, \sqrt{33}$. Jeder Automorphismus von K muß die Eins auf sich selbst abbilden, $\sqrt{3}$ entweder auf sich selbst oder $-\sqrt{3}$, entsprechend auch $\sqrt{11}$ auf sich selbst oder $-\sqrt{11}$. Das Bild von $\sqrt{33}$ muß natürlich das Produkt der Bilder von $\sqrt{3}$ und $\sqrt{11}$ sein. Es gibt somit genau einen Automorphismus $\sigma\colon K \to K$, der $\sqrt{3}$ auf $-\sqrt{3}$ abbildet und $\sqrt{11}$ festläßt, und entsprechend genau einen Automorphismus τ mit $\tau\big(\sqrt{3}\big) = \sqrt{3}$ und $\tau\big(\sqrt{11}\big) = -\sqrt{11}$. Der Fixkörper der von σ und τ erzeugten Gruppe ist $\mathbb{Q}$; somit ist die Körpererweiterung K/Q Galoissch.

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!

Lösung: Die Nullstelle $z = \sqrt{3} + \sqrt{11}$ liegt in K; nach *a)* sind also auch $\sigma(z) = -\sqrt{3} + \sqrt{11}$ und $\tau(z) = \sqrt{3} - \sqrt{11}$ Nullstellen; genauso auch $\sigma\big(\tau(z)\big) = -\sqrt{3} - \sqrt{11}$.

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!

Lösung: Nach *c)* hat jedes solche Polynom f alle vier Zahlen $\pm\sqrt{3} \pm \sqrt{11}$ als Nullstellen, ist also teilbar durch

$$\begin{aligned} g &= (X - \sqrt{3} - \sqrt{11})(X - \sqrt{3} + \sqrt{11})(X + \sqrt{3} - \sqrt{11})(X + \sqrt{3} + \sqrt{11}) \\ &= \Big((X - \sqrt{3})^2 - 11\Big)\Big((X + \sqrt{3})^2 - 11\Big) = (X^2 - 8 - 2\sqrt{3}X)(X^2 - 8 + 2\sqrt{3}X) \\ &= (X^2 - 8)^2 - 12X^2 = X^4 - 28X^2 + 64\,. \end{aligned}$$

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

Lösung: Natürlich liegt L in K. Da g nach *d)* jedes Polynom aus $\mathbb{Q}[X]$ mit $f\big(\sqrt{3}+\sqrt{11}\big) = 0$ teilt, ist $L \cong \mathbb{Q}[X]/(g)$, hat also Grad vier über $\mathbb{Q}$. Denselben Grad hat auch K, also ist $L = K$. Über diesem Körper zerfällt g (nach seiner Konstruktion) in ein Produkt von Linearfaktoren, und über einem echten Teilkörper kann dies nicht der Fall sein, da $\sqrt{3} + \sqrt{11}$ in keinem kleineren Körper als L enthalten ist.

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

Lösung: $L = K$ ist nach *b)* Galoissch; insbesondere liegen die dort konstruierten Automorphismen σ und τ in der Galois-Gruppe. Zusammen mit ihrem Produkt und der Identität bilden sie eine zur Kleinschen Vierergruppe isomorphe Gruppe, und da die Ordnung der Galois-Gruppe gleich dem Grad der Körpererweiterung ist, muß sie die volle Galois-Gruppe sein.