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.

Lösung: Da die Multiplikation mit einem Gruppenelement injektiv ist, gilt

$$[g,h] = ghg^{-1}h^{-1} = e \iff ghg^{-1} = h \iff gh = hg\,.$$

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

Lösung: Wegen $g^2 = e$ ist jedes Element sein eigenes Inverses; für zwei Elemente $g, h \in G$ ist daher

$$[g,h] = ghg^{-1}h^{-1} = ghgh = (gh)^2 = e\,.$$

Nach *a)* ist daher $gh = hg$.

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

Lösung: Da die Konjugation mit x ein Automorphismus von G ist, folgt

$$[g,h]^x = (ghg^{-1}h^{-1})^x = g^x h^x (g^{-1})^x (h^{-1})^x = g^x h^x (g^x)^{-1} (h^x)^{-1} = [g^x, h^x]\,.$$

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

Lösung: Wir müssen zeigen, daß für jedes $n \in [G,G]$ und jedes $x \in G$ auch n^x in $[G,G]$ liegt. n ist ein Produkt von Kommutatoren $[g_i, h_i]$, also ist n^x das Produkt der $[g_i, h_i]^x$. Da dies nach *c)* die Kommutatoren $[g_i^x, h_i^x]$ sind, liegt auch dieses Produkt in $[G,G]$. Somit ist $[G,G]$ ein Normalteiler von G.
$\varphi\colon G \to G/[G,G]$ sei die Abbildung, die jedem Element $g \in G$ seine Restklasse modulo $[G,G]$ zuordnet. Für zwei Elemente $g, h \in G$ ist dann

$$[\varphi(g), \varphi(h)] = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = \varphi(ghg^{-1}h^{-1}) = \varphi([g,h])$$

das Neutralelement von $G/[G,G]$, also kommutieren $\varphi(g)$ und $\varphi(h)$. Da sich jedes Element der Faktorgruppe als Bild eines Elements von G unter φ darstellen läßt, ist diese abelsch.

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 $[\mathfrak{A}_n, \mathfrak{A}_n] = \mathfrak{A}_n$!

Lösung: Nach *d)* ist $[\mathfrak{A}_n, \mathfrak{A}_n]$ ein Normalteiler von $\mathfrak{A}_n$. Wie wir im Zusammenhang mit der Lösbarkeit von Polynomgleichungen durch Radikale gesehen haben, ist $\mathfrak{A}_n$ für $n \geq 5$ eine einfache Gruppe, hat also nur sich selbst und die triviale Gruppe $\{e\}$ als Normalteiler. Wäre die Kommutatorgruppe gleich der trivialen Gruppe, wären alle Kommutatoren von Elementen aus $\mathfrak{A}_n$ trivial, $\mathfrak{A}_n$ wäre also eine abelsche Gruppe. Das ist aber schon für $n \geq 4$ falsch, da beispielsweise $(123)(234) = (12)(34)$, aber $(234)(123) = (13)(24)$ ist. Also muß die Kommutatorgruppe gleich der gesamten Gruppe sein.

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

Lösung: Da bereits die Kommutatoren der Elemente von $\mathfrak{A}_n$ die ganze $\mathfrak{A}_n$ erzeugen, muß $[\mathfrak{S}_n, \mathfrak{S}_n]$ diese Gruppe auf jeden Fall enthalten.
Zwei beliebige Elemente g, h aus $\mathfrak{S}_n$ lassen sich als Produkte von Transpositionen schreiben; für g seien dies p, und für h seien es q Transpositionen. Dann ist auch g^{-1} ein Produkt von p Transpositionen und h^{-1} eines von q; der Kommutator $[g, h]$ läßt sich also schreiben als Produkt von $2(p + q)$ Transpositionen und liegt somit in $\mathfrak{A}_n$. Damit liegt die Kommutatorgruppe in $\mathfrak{A}_n$ und enthält diese Gruppe, ist also gleich $\mathfrak{A}_n$.

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 $e_i \neq 0$.

Lösung: x läßt sich eindeutig darstellen als Quotient z/n zweier teilerfremder Zahlen $z \in \mathbb{Z}$ und $n \in \mathbb{N}$. Dividiert man deren Primfaktorzerlegungen durcheinander und ordnet die Faktoren nach der Größe der Primzahlen, erhält man eine Darstellung der verlangten Art. Sind $x = \pm \prod_{i=1}^{r} p_i^{e_i} = \pm \prod_{j=1}^{r} q_j^{f_j}$ zwei entsprechende Darstellungen, so können wir in beiden Fällen das Produkt aller Potenzen mit positivem Exponenten mal dem Vorzeichen und das inverse Produkt der Potenzen mit negativen Exponenten bilden. Wir erhalten jeweils eine ganze Zahl und eine dazu teilerfremde natürliche Zahl, deren Quotient x ist. Da die Darstellung $x = z/n$ eindeutig ist, ist in beiden Fällen das erste Produkt gleich z und das zweite gleich n; wegen der Eindeutigkeit der Primzerlegung in $\mathbb{Z}$ stehen also in den jeweiligen Produkt in beiden Fällen dieselben Primzahlpotenzen. Da in der Darstellung von x die Primzahlen der Größe nach angeordnet sind, folgt $r = s$ und $p_i = q_i$ für alle i.

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

Lösung: In der Tat: Hätte x in der Darstellung nach *a)* auch Potenzen mit negativen Exponenten, so wäre dies auch bei x^n der Fall; wegen der Eindeutigkeit dieser Darstellung könnte also x keine ganze Zahl sein.

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.

Lösung: Der führende Term von f' ist dX^{d-1} mit $d \geq 2$. Wäre f' ein Teiler von f, so gäbe es ein lineares Polynom $g = aX + b \in \mathbb{Z}[X]$, so daß $f = f'g$ wäre. Insbesondere müßte der führende Koeffizient ad von $f'g$ gleich dem führenden Koeffizienten eins von f sein. Wegen $a, d \in \mathbb{Z}$ und $d \geq 2$ ist das nicht möglich.

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.

Lösung: Hat f in seinem Zerfällungskörper die Nullstellen $x_1, \ldots, x_r$ mit Vielfachheiten $e_1, \ldots, e_r$, so hat f' die Nullstellen $x_1, \ldots, x_r$ mit Vielfachheiten $e_1 - 1, \ldots, e_r - 1$ und keine anderen, da sonst f' kein Teiler von f wäre. Die Summe der $e_i - 1$ muß daher gleich dem Grad $d-1$ von f' sein. Da die Summe der e_i gleich dem Grad d von f ist, ist die der $e_i - 1$ gleich $d-r$; also muß $r = 1$ sein. Wegen des führenden Koeffizienten eins von f folgt daraus, daß $f = (X-a)^d$ ist, also $f' = d(X-a)^{d-1}$. Da f' in $\mathbb{Q}[X]$ ein Teiler von f ist, liegt $f/f' = (X-a)/d$ in $\mathbb{Q}[X]$, d.h. $a \in \mathbb{Q}$. Da der konstante Koeffizient von f gleich $(-a)^d$ ist, muß a nach *b)* eine ganze Zahl sein.

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?

Lösung: Bezeichnet x die Anzahl der Männer, y die der Frauen und z die der Kinder, so gelten die beiden Gleichungen

$$x + y + z = 48 \quad \text{und} \quad 13x + 5y + 2z = 300\,.$$

Auflösen der ersten Gleichung ergibt $z = 48 - x - y$, also ist

$$13x + 5y + 2(48 - x - y) = 11x + 3y + 96 = 300 \quad \text{oder} \quad 11x + 3y = 204\,.$$

Außerdem gelten die Ungleichungen $x \geq 1$, $y \geq 0$, $z \geq 0$ und $y \leq x$.

Da drei ein Teiler von 204 ist, hat die diophantische Gleichung $11x + 3y = 204$ in $\mathbb{Z}$ die Lösung $x = 0$ und $y = 68$; da drei und elf teilerfremd sind und $11 \cdot 3 - 3 \cdot 11$ verschwindet, ist die allgemeine Lösung daher $x = 3k$ und $y = 68 - 11k$ mit einer beliebigen ganzen Zahl k. Für $k > 6$ wird y negativ, also muß $k \leq 6$ sein, und natürlich ist $k \geq 1$.

Die Anzahl $z = 48 - x - y = 48 - 3k - 68 + 11k = 8k - 20$ der Kinder kann auch nicht negativ sein, also muß $k \geq 3$ sein. Schließlich ist noch

$$y = 68 - 11k \leq x = 3k \Longrightarrow 68 \leq 14k \Longrightarrow k \geq 5\,.$$

Also kommen nur $k = 5$ und $k = 6$ infrage. $k = 5$ führt zu der Lösung $x = 15, y = 13$ und $z = 20$, während $k = 6$ auf $x = 18, y = 2$ und $z = 28$ führt. Beides ist grundsätzlich möglich; da es aber heutzutage eher unwahrscheinlich ist, daß zwei Paare zusammen 28 Kinder haben, spricht vieles für die erste Lösung mit 15 Männern, 13 Frauen und 20 Kindern.

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?

Lösung: *Ja,* denn $15 = 5 \cdot 3 = (2^2+1)(2+1)$ ist das Produkt zweier Fermatscher Primzahlen, so daß das Fünfzehneck mit Zirkel und Lineal konstruierbar ist. Das Achtzehneck ist nicht mit Zirkel und Lineal konstruierbar, denn $18 = 2 \cdot 3^2$ enthält die ungerade Primzahl drei mehrfach.

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: $U(xy) = U(x)U(y)$.

Lösung: Die RSA-Unterschrift unter eine Nachricht x ist $U(x) = x^d \bmod N$. Für zwei Nachrichten x, y ist daher in $\mathbb{Z}/N$

$$U(xy) = (xy)^d \bmod N = (x^d y^d) \bmod N = (x^d \bmod N)(y^d \bmod N) = U(x)U(y)\,.$$

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?

Lösung: $\varphi(mz^e) = \varphi(m)\varphi(z^e) = \varphi(m)z$, denn φ und die Verschlüsselungsfunktion $x \mapsto x^e \bmod N$ sind invers zueinander. Somit muß mit dem erweiterten EUKLIDischen Algorithmus ein Inverses z^{-1} von z modulo N berechnet werden. Damit läßt sich dann $\varphi(m) = \varphi(mz^e)z^{-1} \bmod N$ durch eine modulare Multiplikation berechnen.

Aufgabe 5: (*4 Punkte*)

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

Lösung: In $\mathbb{Q}[X]$ ist 21 eine Einheit; wenn wir sie ausklammern bleibt $X^3 - 1$ übrig. Offensichtlich ist eins eine Nullstelle; $(X^3-1) : (X-1) = X^2+X+1$ ist über $\mathbb{Q}$ irreduzibel, da die Nullstellen $-\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$ irrational sind und ein reduzibles quadratisches Polynom zwei lineare Faktoren haben müßte. In $\mathbb{Q}[X]$ ist also $f = 21(X-1)(X^2+X+1)$.
In $\mathbb{Z}[X]$ sind nur ± 1 Einheiten; 21 kann zerlegt werden in das Produkt der beiden Primzahlen drei und sieben. Somit ist dort $f = 3 \cdot 7 \cdot (X-1) \cdot (X^2+X+1)$ die Zerlegung in irreduzible Faktoren.

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

Lösung: Da die Nullstellen des quadratischen Faktors in $\mathbb{Q}[\sqrt{-3}]$ liegen, können wir diesen weiter zerlegen und erhalten $f = 21(X-1)\big(X+\frac{1}{2}+\frac{1}{2}\sqrt{-3}\big)\big(X+\frac{1}{2}-\frac{1}{2}\sqrt{-3}\big)$.

Aufgabe 6: (*12 Punkte*)

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

Lösung: Da die vierte Potenz von $\sqrt[4]{5}$ in $\mathbb{Q}$ liegt, bilden die niedrigeren Potenzen eine solche Basis; als $\mathbb{Q}$-Vektorraum ist also $K = \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \sqrt[4]{5} \oplus \mathbb{Q} \cdot \sqrt{5} \oplus \mathbb{Q} \cdot 5^{3/4}$.
Ein Automorphismus von $K/\mathbb{Q}$ läßt $\mathbb{Q}$ fest und bildet $\sqrt[4]{5}$ ab auf eine Nullstelle des Polynoms $X^4 - 5$. Abgesehen von $\sqrt[4]{5}$ ist $-\sqrt[4]{5}$ die einzige weitere Nullstelle in K; außer der Identität gibt es also nur noch den Automorphismus, der $\sqrt[4]{5}$ auf $-\sqrt[4]{5}$ abbildet. $\sqrt{5}$ als Quadrat von $\sqrt[4]{5}$ bleibt invariant, und $5^{3/4}$ geht auf $-5^{3/4}$. $\mathrm{Aut}(K/Q)$ ist die von diesem Automorphismus erzeugte zyklische Gruppe der Ordnung zwei.

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

Lösung: Das Polynom hat die vier Nullstellen $\pm\sqrt[4]{5}$ und $\pm i\sqrt[4]{5}$; der Zerfällungskörper wird also erzeugt von $\sqrt[4]{5}$ und $i\sqrt[4]{5}$. Er enthält damit auch den Quotienten i dieser beiden

Zahlen, und da $i\sqrt[4]{5}$ als Produkt von i und $\sqrt[4]{5}$ in $\mathbb{Q}(\sqrt[4]{5}, i)$ liegt, erzeugen $\sqrt[4]{5}$ und i denselben Körper wie $\sqrt[4]{5}$ und $i\sqrt[4]{5}$.

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

Lösung: Nach *b)* ist $L = K(i) = K \cdot 1 \oplus K \cdot i$; also ist $\{1, i\}$ eine K-Vektorraumbasis. Für eine $\mathbb{Q}$-Vektorraumbasis können wir die vier Elemente aus *a)* nehmen sowie ihre Produkte mit i, also ist

$$L = K \cdot 1 \oplus K \cdot i = \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \sqrt[4]{5} \oplus \mathbb{Q} \cdot \sqrt{5} \oplus \mathbb{Q} \cdot 5^{3/4} \oplus \mathbb{Q} \cdot i \oplus \mathbb{Q} \cdot i\sqrt[4]{5} \oplus \mathbb{Q} \cdot i\sqrt{5} \oplus \mathbb{Q} \cdot i5^{3/4} .$$

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!

Lösung: $\sigma(\sqrt[4]{5}) = i\sqrt[4]{5}$, $\sigma(i\sqrt[4]{5}) = -\sqrt[4]{5}$, $\sigma(-\sqrt[4]{5}) = -i\sqrt[4]{5}$ und $\sigma(-i\sqrt[4]{5}) = \sqrt[4]{5}$. Viermalige Anwendung von σ auf $\sqrt[4]{5}$ führt also erstmalig zurück zum Ausgangspunkt. Da jedes Element von K als rationales Polynom in $\sqrt[4]{5}$ geschrieben werden kann und σ^4, genau wie σ, auf $\mathbb{Q}$ trivial operiert, ist σ^4 auf ganz K gleich der Identität, d.h. σ hat die Ordnung vier.

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!

Lösung: Da die komplexe Konjugation mit allen Grundrechenarten vertauschbar ist und L zu jedem Element auch dessen konjugiert komplexes enthält, ist τ ein Automorphismus von $L/\mathbb{Q}$ (und auch von L/K). Ein allgemeines Element $x \in L$ läßt sich nach *c)* eindeutig schreiben als $x = a_1 + a_2\sqrt[4]{5} + a_3\sqrt{5} + a_4 5^{3/4} + a_5 i + a_6 i\sqrt[4]{5} + a_7 i\sqrt{5} + a_8 i5^{3/4}$; beim komplex konjugierten Element $\tau(x)$ werden a_5 bis a_8 durch ihr Negatives ersetzt. Falls $\tau(x) = x$ sei soll, müssen diese Koeffizienten daher verschwinden; der Fixkörper von τ ist also K. Wenn wir auf $x = a_1 + a_2\sqrt[4]{5} + a_3\sqrt{5} + a_4 5^{3/4} \in K$ den Automorphismus σ anwenden, erhalten wir $\sigma(x) = a_1 + a_2 i\sqrt[4]{5} - a_3\sqrt{5} - a4i5^{3/4}$; dies ist genau dann gleich x, wenn $a_2 = a_3 = a_4 = 0$ ist. Der Fixkörper von $\{\sigma, \tau\}$ ist daher $\mathbb{Q}$.
Da $[K : \mathbb{Q}] = 8$ ist, hat $\mathrm{Aut}(K/Q)$ acht Elemente. Dazu gehören σ und τ. Für sich allein erzeugt σ nach *d)* eine zyklische Gruppe der Ordnung vier, die τ nicht enthält. Nehmen wir τ dazu, erhalten wir eine größere Untergruppe von $\mathrm{Aut}(K/\mathbb{Q})$, deren Ordnung größer vier und nach LAGRANGE ein Teiler von acht sein muß. Also hat diese Gruppe acht Elemente ist damit gleich $\mathrm{Aut}(K/\mathbb{Q})$.

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

Lösung: Wegen $L = K(i) = K \oplus Ki$ ist das natürlich die von der komplexen Konjugation erzeugte zyklische Gruppe der Ordnung zwei.