Universität Konstanz
Fachbereich Mathematik und Statistik

Markus Schweighofer
30. März 2011

Klausur zur Einführung in die Algebra (Modulklausur, Zwischenprüfung)

Familienname: Connes

Vorname: Alain

Matrikelnummer: 01041947

Übungsgruppenleiter: Jacques Dixmier

Aufgabe	1	2	3	4	5	6	7	$\sum$
erreichte Punktzahl	8	16	8	10	20	8	30	100
Korrektor (Initialen)	XY	XY	XY	XY	XY	XY	XY	XY
Maximalpunktzahl	8	16	8	10	20	8	30	100

Fassen Sie den Klausurbogen nicht an, bevor die Klausur eröffnet wird!

Entfernen Sie nicht die Klammerung der Blätter. Sobald die Klausur eröffnet wird, tragen Sie auf **jeder Vorderseite sofort** Ihren Namen ein. Schreiben Sie die Lösung zu einer Aufgabe nur auf die dafür vorgesehenen Blätter. Wenn Sie sich nicht ganz sicher sind und noch genug Zeit ist, empfiehlt es sich, die Lösung zunächst auf Schmierpapier zu schreiben. Vergessen Sie aber nicht, die Lösung rechtzeitig auf den Klausurbogen zu übertragen. Soweit nichts anderes gesagt ist, gilt folgendes:

- Alle Antworten sind mathematisch zu begründen.
- Sofern nichts anderes gesagt ist, darf dabei auf mathematische Ergebnisse aus der Vorlesung und der Übung zur Einführung in die Algebra (WS 2010/2011) verwiesen werden (zum Beispiel durch ein Stichwort wie „Hauptsatz der Galoistheorie“ oder durch kurze Beschreibung des Ergebnisses).
- Sie können die einzelnen Teilaufgaben einer Aufgabe in einer anderen als der vorgeschlagenen Reihenfolge bearbeiten und in jeder Teilaufgabe die erzielten (Zwischen-)Ergebnisse aus den vorher bearbeiteten Teilaufgaben verwenden.

Haben Sie irgendwelche Fragen, so zögern Sie nicht, sich (möglichst lautlos) bemerkbar zu machen. Ein Mitarbeiter wird zu Ihnen an den Platz kommen.

Die maximale Bearbeitungszeit beträgt 180 Minuten. Die einzigen erlaubten Hilfsmittel sind “Spickzettel”[1], Schreibzeug, Schmierpapier[2] und eine Uhr[3]. Viel Erfolg!

[1] ein beidseitig von eigener Hand beschriebenes Blatt im Format A4
[2] anfangs unbeschrieben
[3] ohne eingebaute Kommunikationsgeräte

Name: Alain Connes **Seite 1 zur Aufgabe 1**

erreichte Punktzahl: 8 **Korrektor (Initialen): XY**

Aufgabe 1 (8 Punkte). Sei G eine Gruppe und H eine nichtleere **endliche** Teilmenge, die unter der Gruppenmultiplikation abgeschlossen ist, das heißt es gilt $\emptyset \neq H \subseteq G$ und für alle $a,b \in H$ gilt $ab \in H$. Ist dann H stets eine Untergruppe von G? Gebe einen Beweis oder finde ein Gegenbeispiel!

Lösung zur Aufgabe 1: Ja, H ist in der Tat stets eine Untergruppe von G. Hierzu reicht es zu zeigen:

(a) $a^{-1} \in H$ für alle $a \in H \setminus \{1\}$

(b) $1 \in H$

Zu (a). Sei $a \in H \setminus \{1\}$. Aus der Voraussetzung folgt per Induktion sofort $a^k \in H$ für alle $k \in \mathbb{N}$. Da H endlich ist, gibt es $k,\ell \in \mathbb{N}$ mit $k < \ell$ und $a^k = a^\ell$. Indem man mit a^{-k} multipliziert, sieht man, dass es ein $n \in \mathbb{N}$ gibt mit $a^n = 1$. Wegen $a \neq 1$ gilt $n \geq 2$ und es folgt $a^{-1} = a^{n-1} \in H$.

Zu (b). Nach Voraussetzung können wir ein $a \in H$ wählen. Gilt $a = 1$, so sind wir fertig. Sonst gilt aber nach (a), dass $a^{-1} \in H$ und daher $1 = aa^{-1} \in H$.

Name: Alain Connes **Seite 1 zur Aufgabe 2**

erreichte Punktzahl: 16 **Korrektor (Initialen): XY**

Aufgabe 2 (16 Punkte). Sei G eine Gruppe von ungerader Ordnung und

$$f\colon G \to G,\ a \mapsto a^2.$$

(a) Zeige, dass f ein *Gruppenautomorphismus* ist, wenn G sogar eine abelsche Gruppe ist.

(b) Finde eine Gruppe G ungerader Ordnung und $a,b \in G$ mit $f(ab) \neq f(a)f(b)$.

(c) Zeige, dass für alle $a \in G$ die Elemente a und a^2 dieselbe Untergruppe erzeugen, das heißt

$$\langle a\rangle = \langle a^2\rangle.$$

(d) Zeige, dass f immer eine *bijektive Abbildung* ist.

Lösung zur Aufgabe 2: (a) Ist G abelsch, so gilt für alle $a,b \in G$

$$f(ab) = (ab)^2 = abab = aabb = a^2b^2 = f(a)f(b),$$

das heißt f ist ein Gruppenhomomorphismus. Es ist noch zu zeigen, daß f bijektiv ist. Da G endlich ist, reicht es hierzu zu zeigen, dass f injektiv ist, was gleichbedeutend mit $\ker f = \{1\}$ ist. Sei also $a \in G$ mit $f(a) = 1$. Zu zeigen ist $a = 1$. Wäre $a \neq 1$, so hätte a wegen $a^2 = f(a) = 1$ die Ordnung 2 in G, womit die von a erzeugte Untergruppe $\langle a\rangle$ die Ordnung 2 hätte, was nach dem Satz von Lagrange im Widerspruch zur Voraussetzung steht, dass $\#G$ ungerade ist.

(b) Nehme für G zum Beispiel die aus der Vorlesung bekannte Gruppe der oberen unipotenten 3×3-Dreiecksmatrizen über $\mathbb{F}_3$, also

$$G = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\} \leq \mathrm{GL}_3(\mathbb{F}_3).$$

Offensichtlich ist $\#G = 3^3$ ungerade. Setze nun

$$a := \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad b := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Dann gilt

$$a^2 = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad b^2 = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

sowie

$$ab = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad (ab)^2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Daher

$$f(ab) = (ab)^2 \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = a^2b^2 = f(a)f(b).$$

(c) Da mit G nach dem Satz von Lagrange auch die Untergruppe $\langle a\rangle$ von G ungerade Ordnung hat und $\langle a\rangle$ abelsch (sogar zyklisch) ist, ist nach (a) die Abbildung

$$g\colon \langle a\rangle \to \langle a\rangle,\ b \mapsto b^2$$

ein Gruppenautomorphismus. Insbesondere gilt $\langle a\rangle = g(\langle a\rangle) = \langle g(a)\rangle = \langle a^2\rangle$.

(d) Da G endlich ist, reicht es zu zeigen, dass f surjektiv ist. Sei hierzu $a \in G$. Dann gilt

$$a \in \langle a\rangle \overset{(c)}{=} \langle a^2\rangle = \langle f(a)\rangle \leq \operatorname{im} f,$$

also $a \in \operatorname{im} f$.

Name: Alain Connes **Seite 1 zur Aufgabe 3**

erreichte Punktzahl: 8 **Korrektor (Initialen): XY**

Aufgabe 3 (8 Punkte). Zeige, dass das Polynom $X^3 + 3X + 1$ irreduzibel in $\mathbb{Q}[X]$ ist.

Lösung zur Aufgabe 3: Wir wenden das Reduktionskriterium an: Es gilt $\mathbb{Q} = \mathrm{qf}(\mathbb{Z})$ und $\mathbb{Z}$ ist faktoriell. Da 2 irreduzibel in $\mathbb{Z}$ ist und der Leitkoeffizient des Polynoms X^3+3X+1 vom Grad ≥ 1 nicht von 2 geteilt wird, reicht es zu zeigen, dass $X^3+X+1 = X^3+3X+1$ in $(\mathbb{Z}/(2))[X] = \mathbb{F}_2[X]$ irreduzibel ist. Da dies ein Polynom vom Grad 3 ist, reicht es zu zeigen, dass es keine Nullstelle in $\mathbb{F}_2$ hat, was man sofort sieht.

Name: Alain Connes **Seite 1 zur Aufgabe 4**

erreichte Punktzahl: 10 **Korrektor (Initialen): XY**

Aufgabe 4 (10 Punkte). Sei $S := \{3^k \mid k \in \mathbb{N}_0\} \subseteq \mathbb{Z}$. Finde ein Polynom $f \in \mathbb{Z}[X]$ derart, dass die Ringe $S^{-1}\mathbb{Z}$ und $\mathbb{Z}[X]/(f)$ isomorph sind. (Die Isomorphie ist selbstverständlich nachzuweisen.)

Lösung zur Aufgabe 4: Setze $f := 3X - 1 \in \mathbb{Z}[X]$.

Der eindeutig bestimmte Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}[X]/(f)$ bildet 3 auf $\overline{3}$ ab, was wegen $\overline{3}\,\overline{X} = \overline{3X} = 1$ eine Einheit im Ring $\mathbb{Z}[X]/(f)$ ist. Damit bildet dieser Homomorphismus aber offensichtlich jedes Element von S auf eine Einheit ab und kann daher zu einem Ringhomomorphismus

$$\varphi\colon S^{-1}\mathbb{Z} \to \mathbb{Z}[X]/(f),\ \frac{a}{3^k} \mapsto \frac{\overline{a}}{\overline{3}^k} = \overline{aX^k} \qquad (a \in \mathbb{Z}, k \in \mathbb{N}_0)$$

fortgesetzt werden.

Umgekehrt liegt f im Kern des Einsetzungshomomorphismus $\mathbb{Z}[X] \to S^{-1}\mathbb{Z}$, $p \mapsto p(\frac{1}{3})$, was mit Homomorphiesatz den Ringhomomorphismus

$$\psi\colon \mathbb{Z}[X]/(f) \to S^{-1}\mathbb{Z},\ \overline{p} \mapsto p(\frac{1}{3}) \qquad (p \in \mathbb{Z}[X])$$

liefert. Es gilt

$$(\varphi \circ \psi)(\overline{p}) = \varphi(\psi(\overline{p})) = \varphi(p(\frac{1}{3}))) = \overline{p}$$

für alle $p \in \mathbb{Z}[X]$ und

$$(\psi \circ \varphi)(\frac{a}{3^k}) = \psi(\varphi(\frac{a}{3^k})) = \psi(\overline{aX^k}) = \frac{a}{3^k}$$

für alle $a \in \mathbb{Z}$ und $k \in \mathbb{N}_0$. Dies zeigt

$$\varphi \circ \psi = \mathrm{id}_{\mathbb{Z}[X]/(f)}$$

und

$$\psi \circ \varphi = \mathrm{id}_{S^{-1}\mathbb{Z}}\,.$$

Somit sind φ und ψ Isomorphismen.

Name: Alain Connes **Seite 1 zur Aufgabe 5**

erreichte Punktzahl: 20 **Korrektor (Initialen): XY**

Aufgabe 5 (20 Punkte). Betrachte die Ringe

$$A_1 := \mathbb{Z}/(25), A_2 := \mathbb{F}_{25}, A_3 := \mathbb{F}_5[X]/(X^2+1), A_4 := \mathbb{F}_5[X]/(X^2+X+1) \text{ und } A_5 := \mathbb{F}_5 \times \mathbb{F}_5.$$

Für welche $(i,j) \in \{1,\dots,5\}^2$ mit $i < j$ sind die Ringe A_i und A_j isomorph und für welche nicht? Begründe Deine Antwort.

Lösung zur Aufgabe 5: A_4 ist ein Körper. Nach Korollar 2.4.9 aus der Vorlesung folgt dies daraus, dass $\mathbb{F}_5[X]$ ein Hauptidealring ist und X^2+X+1 irreduzibel in $\mathbb{F}_5[X]$ ist. Ersteres ist klar, denn $\mathbb{F}_5$ ist ein Körper und letzteres folgt daraus, dass X^2+X+1 keine Nullstelle in $\mathbb{F}_5$ hat. Wegen $\#A_4 = 25$ (A_4 ist ein $\mathbb{F}_5$-Vektorraum mit zweielementiger Basis $\overline{1},\overline{X}$) ist A_4 genauso wie A_2 ein 25-elementiger Körper. Nach Korollar 4.4.15(b) aus der Vorlesung sind zwei gleichmächtige endliche Körper schon isomorph, das heißt es gilt

$$A_2 \cong A_4.$$

Im Hinblick auf A_3, betrachten wir als nächstes das Polynom $X^2+1 \in \mathbb{F}_5[X]$. Es sind $2,3 \in \mathbb{F}_5$ Nullstellen dieses Polynoms, woraus in $\mathbb{F}_5[X]$ folgt $X^2+1 = (X-2)(X-3)$. Da $X-2$ und $X-3$ selbstverständlich nicht assoziiert und irreduzibel sind in $\mathbb{F}_5[X]$, folgt aus dem (Korollar 2.8.6 zum) Chinesischen Restsatz, dass $A_3 = \mathbb{F}_5[X]/(X^2+1) \cong (\mathbb{F}_5[X]/(X-2)) \times (\mathbb{F}_5[X]/(X-3)) = \mathbb{F}_5 \times \mathbb{F}_5 = A_5$, also

$$A_3 \cong A_5$$

(die dabei benutzte Isomorphie $\mathbb{F}_5[X]/(X-a) \cong \mathbb{F}_5$ für $a \in \mathbb{F}_5$ erhält man sofort durch Anwendung des Isomorphiesatzes auf den Einsetzungshomomorphismus $\mathbb{F}_5[X] \to \mathbb{F}_5$, $f \mapsto f(a)$).

Der Ring A_1 hat die Charakteristik 25, während alle anderen A_i die Charakteristik 5 haben. Insbesondere ist A_1 zu keinem der anderen Ringe isomorph. Wir merken uns also:

$$A_1 \ncong A_2, \qquad A_1 \ncong A_3.$$

Schließlich ist $A_5 \cong A_3$ kein Körper, da $(0,1) \in A_5 \setminus \{0\}$ offensichtlich keine Einheit ist. Also

$$A_2 \ncong A_3.$$

Zusammenfassend erhält man also:

	A_1	A_2	A_3	A_4	A_5
A_1		$\ncong$	$\ncong$	$\ncong$	$\ncong$
A_2			$\ncong$	$\cong$	$\ncong$
A_3				$\ncong$	$\cong$
A_4					$\ncong$
A_5					

Name: Alain Connes **Seite 1 zur Aufgabe 6**

erreichte Punktzahl: 8 **Korrektor (Initialen): XY**

Aufgabe 6 (8 Punkte). Sei $L|K$ eine Körpererweiterung vom Grad $[L : K] = 2^k$ für ein $k \in \mathbb{N}_0$. Sei $f \in K[X]$ ein Polynom vom Grad 3, das in L eine Nullstelle besitzt. Besitzt dann f bereits in K eine Nullstelle? Gebe einen Beweis oder ein Gegenbeispiel!

Lösung zur Aufgabe 6: Ja, f besitzt dann in K eine Nullstelle. Wir zeigen dies durch Widerspruch und nehmen daher an, dies ist nicht so. Da f vom Grad 3 ist, ist f dann irreduzibel in $K[X]$. Wähle nun gemäß Voraussetzung ein $a \in L$ mit $f(a) = 0$. Ohne Einschränkung sei f normiert. Dann ist f das Minimalpolynom von a über K und daher $[K(a) : K] = \deg f = 3$. Nun gilt mit der Gradformel $2^k = [L : K] = [L : K(a)][K(a) : K] = 3[L : K(a)]$, was absurd ist.

Name: Alain Connes **Seite 1 zur Aufgabe 7**

erreichte Punktzahl: 30 **Korrektor (Initialen): XY**

Aufgabe 7 (30 Punkte). Sei L der Zerfällungskörper des Polynoms $f := X^3 + 2X - 1 \in \mathbb{Q}[X]$ über $\mathbb{Q}$.

(a) Begründe, warum $L|\mathbb{Q}$ eine endliche Galoiserweiterung ist.

(b) Begründe mit Hilfe von Analysis, warum f genau eine reelle Nullstelle $a_1 \in \mathbb{R}$ hat.

(c) Zeige, dass f irreduzibel in $\mathbb{Q}[X]$ ist.

Hinweis: Man kann *zum Beispiel* das Reduktionskriterium verwenden.

(d) Begründe, warum es a_2,$a_3 \in \mathbb{C} \setminus \mathbb{R}$ gibt mit $f = (X - a_1)(X - a_2)(X - a_3)$.

(e) Begründe, warum es $\varphi \in \mathrm{Aut}(L|\mathbb{Q})$ gibt mit $\varphi(a_1) = a_2$.

(f) Bestimme $G := \mathrm{Aut}(L|\mathbb{Q})$ als Untergruppe von S_3.

Hinweis: Zeige zunächst $(2\ 3) \in G$ und benutze dann (e).

(g) Bestimme $[L : \mathbb{Q}]$.

(h) Bestimme alle Untergruppen von $\mathrm{Aut}(L|\mathbb{Q})$.

(i) Bestimme *die Anzahl* der Zwischenkörper von $L|\mathbb{Q}$.

(j) Bestimme $[K : \mathbb{Q}]$ für den Zwischenkörper $K := \mathbb{Q}(x)$ von $L|\mathbb{Q}$ mit

$$x := (a_1 - a_2)(a_2 - a_3)(a_3 - a_1).$$

Lösung zur Aufgabe 7: (a) Als Zerfällungskörper eines Polynoms über $\mathbb{Q}$ ist $L|\mathbb{Q}$ eine endliche normale Erweiterung. Da $\mathbb{Q}$ Charakteristik 0 hat, ist $\mathbb{Q}$ vollkommen, das heißt jede endliche (oder sogar algebraische) Erweiterung von $\mathbb{Q}$ ist separabel über $\mathbb{Q}$. Da $L|\mathbb{Q}$ also normal und separabel ist, ist es galoissch.

(b) Die Ableitung $f' = 3X^2 + 2$ nimmt auf ganz $\mathbb{R}$ nur positive Werte an positiv, weswegen mit Analysis f auf $\mathbb{R}$ streng monoton steigt. Daher hat f höchstens eine reelle Nullstelle. Nach dem Zwischenwertsatz aus der Analysis hat f andererseits mindestens eine reelle Nullstelle, denn $f(0) = -1 < 0$ und $f(1) = 2 > 0$.

(c) Es ist $\mathbb{Q} = \mathrm{qf}(\mathbb{Z})$, $\mathbb{Z}$ faktoriell, $f \in \mathbb{Z}[X]$ ein Polynom vom Grad ≥ 1, dessen Leitkoeffizient nicht von dem irreduziblen Element $3 \in \mathbb{Z}$ geteilt wird. Nach dem Reduktionskriterium reicht es daher zu zeigen, dass $X^3 + 2X - 1 \in \mathbb{F}_3[X]$ irreduzibel in $(\mathbb{Z}/(3))[X] = \mathbb{F}_3[X]$ ist. Dies folgt aber sofort daraus, dass es ein Polynom vom Grad 3 ohne Nullstelle in $\mathbb{F}_3$ ist.

(d) Nach dem Fundamentalsatz der Algebra (und der Normiertheit von f), gibt es a_2,$a_3 \in \mathbb{C}$ mit $f = (X - a_1)(X - a_2)(X - a_3)$. Wäre die nach (b) eindeutige reelle Nullstelle a_1 von f eine mehrfache Nullstelle von f, so wäre sie auch eine Nullstelle von $f' = 3X^2 + 2$, was nicht möglich ist, wie in (b) bereits bemerkt wurde. Also sind weder a_2 noch a_3 reell.

(e) Aus (c) folgt, dass f sowohl das Minimalpolynom von a_1 als auch von a_2 (sowie von a_3) über $\mathbb{Q}$ ist. Mit Proposition 4.3.11 aus der Vorlesung bedeutet das, dass a_1 und a_2 über K konjugiert sind, in Zeichen $a_1 \sim_K a_2$. Es gibt also einen Automorphismus ψ von $\overline{L}|K$ mit $\psi(a_1) = a_2$ (beachte, dass der algebraische Abschluss $\overline{L}$ von L auch ein algebraischer Abschluss von K ist, da $L|K$ algebraisch ist). Da $L|K$ normal ist, gilt $\psi(L) = L$ nach Satz 4.3.14, woraus folgt, dass $\varphi := \psi|_L$ ein Automorphismus von $L|K$ ist mit $\varphi(a_1) = a_2$.

Seite 2 zur Aufgabe 7

Fortsetzung der Lösung zur Aufgabe 7: (f) Die komplexe Konjugation $\mathbb{C} \to \mathbb{C}$, $z \mapsto z^*$ ist ein Automorphismus von $\mathbb{C}|\mathbb{Q}$. Sie permutiert die Nullstellen a_1, a_2 und a_3 von $f \in \mathbb{Q}[X]$. Dabei gilt $a_1^* = a_1$ (da $a_1 \in \mathbb{R}$), $a_2^* = a_3$ (denn $a_2^* \neq a_1$ wegen $a_1 \in \mathbb{R}$ und $a_2 \in \mathbb{C} \setminus \mathbb{R}$ und $a_2^* \neq a_2$ wegen $a_2 \notin \mathbb{R}$) und somit auch $a_3^* = a_2$. Daher bildet sie auch $L = \mathbb{Q}(a_1,a_2,a_3)$ auf $\mathbb{Q}(a_1^*,a_2^*,a_3^*) = \mathbb{Q}(a_1,a_3,a_2) = \mathbb{Q}(a_1,a_2,a_3) = L$ ab und vermittelt daher den Automorphismus $(2\ 3) \in G$.

Aus (e) folgt weiterhin, dass $(1\ 2) \in G$ oder $(1\ 2\ 3) \in G$. In ersterem Fall gilt ebenfalls $(1\ 2\ 3) = (1\ 2)(2\ 3) \in G$. In jedem Fall haben wir also $(1\ 2\ 3),(2\ 3) \in G$, so dass $G \leq S_3$ sowohl ein Element der Ordnung 2 als auch der Ordnung 3 enthält. Somit wird die Gruppenordnung von G sowohl von 2 als auch von 3 und somit von 6 geteilt. Also $6 \leq \#G \leq \#S_3 = 3! = 6$ und daher

$$G = S_3.$$

(g) Mit Galoistheorie folgt $[L : \mathbb{Q}] = \#G \overset{(f)}{=} \#S_3 = 6$.

(h) Nach (f) sind alle Untergruppen von S_3 zu bestimmen. Dies sind offensichtlich

$$\{1\}, \qquad \langle(1\ 2)\rangle, \qquad \langle(1\ 3)\rangle, \qquad \langle(2\ 3)\rangle, \qquad A_3 = \langle(1\ 2\ 3)\rangle \quad \text{und} \quad S_3.$$

(i) Nach Galoistheorie ist die Anzahl der Zwischenkörper von $L|\mathbb{Q}$ gleich der Anzahl der Untergruppen von G, also 6 nach (h).

(j) Setzt man $\varphi := (1\ 2\ 3) \in G$, so gilt $\varphi(x) = (\varphi(a_1)-\varphi(a_2))(\varphi(a_2)-\varphi(a_3))(\varphi(a_3)-\varphi(a_1)) = (a_2-a_3)(a_3-a_1)(a_1-a_2) = (a_1-a_2)(a_2-a_3)(a_3-a_1) = x$. Wegen $\langle\varphi\rangle = A_3$ folgt daher $x \in L^{A_3}$. Mit dem Hauptsatz der Galoistheorie folgt $[L^{A_3} : \mathbb{Q}] = [L^{A_3} : L^{S_3}] = [S_3 : A_3] = 2$. Es gilt also

$$2 \overset{x\notin\mathbb{Q}}{\leq} [\mathbb{Q}(x) : \mathbb{Q}] \overset{x\in L^{A_3}}{\leq} [L^{A_3} : \mathbb{Q}] = 2,$$

und daher

$$[\mathbb{Q}(x) : \mathbb{Q}] = 2.$$

Hierbei muss man noch $x \notin \mathbb{Q}$ nachweisen, was zum Beispiel daraus folgt, dass für $\psi := (2\ 3) \in G$ gilt $\psi(x) \neq x$, denn

$$\begin{aligned}\psi(x) &= (\psi(a_1) - \psi(a_2))(\psi(a_2) - \psi(a_3))(\psi(a_3) - \psi(a_1)) \\ &= (a_1 - a_3)(a_3 - a_2)(a_2 - a_1) = (-1)^3(a_1 - a_2)(a_2 - a_3)(a_3 - a_1) = -x \neq x.\end{aligned}$$