WOLFGANG K. SEILER
*Tel.* 2515

B6,26, A4.18

*27. Februar 2021*

# Modulklausur Algebra

**Aufgabe 1:** (*7 Punkte*)

*a)* Bestimmen Sie alle komplexen Lösungen der Gleichung $x^2 + 6x - 3 = 8i(x + 3)$!

**Lösung:** Bringt man alle mit $x$ behafteten Terme auf die linke Seite und den Rest auf die rechte, wir die Gleichung zu $x^2 + (6 - 8i)x = 3 + 24i$ (d.h. $p = 6 - 8i$ und $q = -3 - 24i$) oder $\big(x-(3-4i)\big)^2-(3-4i)^2 = \big(x+(3-4i)\big)^2+7+24i = 3+24i$. Subtraktion von $7+24i$ auf beiden Seiten macht daraus $\big(x+(3-4i)\big)^2 = -4$, d.h. $x+(3-4i) = \pm 2i$. Die Lösungen sind somit $-3 + 2i$ und $-3 + 6i$.

*b)* Bestimmen Sie über den Satz von VIÈTE alle komplexen Lösungen der Gleichung $x^2 + 4x = 3i(4 + x)$!

**Lösung:** Nach $x$-Potenzen sortiert wird die Gleichung zu $x^2 + (4 - 3i)x - 12i = 0$, d.h. $p = 4 - 3i$ und $q = -12i$ für die Form $x^2 + px + q = 0$. Nach dem Satz von VIÈTE ist die Summe der beiden Lösungen gleich $-p = -4 + 3i$ und das Produkt ist $q = -12i$. Es ist klar, daß nur die beiden Lösungen $x = -4$ und $x = 3i$ in Frage kommen.

*c)* Bestimmen Sie zunächst alle ganzzahligen, dann alle komplexen Nullstellen (einschließlich Vielfachheit) der Gleichung $x^5 - 8x^3 + 2x^2 + 15x = 10$!

**Lösung:** Sei $f(x) = x^5 - 8x^3 + 2x^2 + 15x - 10$. Die ganzzahligen Nullstellen von $f$ sind Teiler des konstanten Terms $-10$, also kommen höchstens $\pm 1, \pm 2, \pm 5$ und $\pm 10$ in Frage. $f(1) = 0$, $f(-1) = -16$, $f(2) = -4$, $f(-2) = 0$, $f(5) = 2240$, $f(-5) = -2160$, $f(10) = 92340$ und $f(-10) = -91960$. (Bei $\pm 5$ und $\pm 10$ ist eigentlich auch ohne Rechnung klar, daß der Term $x^5$ von den anderen nicht mehr kompensiert werden kann.)
Somit sind $1$ und $-2$ die einzigen ganzzahligen Nullstellen.
$f'(x) = 5x^4 - 24x^2 + 4x + 15$ hat bei $x = 1$ den Wert Null und bei $x = 2$ den Wert vier, also ist nur die Eins eine mehrfache Nullstelle. $f''(x) = 20x^3 - 48x + 4$ hat dort den Wert $-24$, also handelt es sich um eine doppelte Nullstelle. Damit kennen wir drei Nullstellen; ihre Summe ist $1 + 1 - 2 = 0$, und ihr Produkt ist $-2$. Die Summe aller Nullstellen ist ebenfalls Null, da es keinen Term mit $x^4$ gibt, und ihr Produkt ist zehn. Die beiden restlichen Nullstellen sind somit $\pm\sqrt{5}$ jeweils mit Vielfachheit eins, da die Summe aller Vielfachheiten nicht größer als der Grad fünf sein kann.

**Aufgabe 2:** (*6 Punkte*)

Eine Untergruppe $U$ einer Gruppe $G$ heißt *charakteristische Untergruppe* von $G$, wenn für jeden Automorphismus $\varphi\colon G \to G$ gilt: $\varphi(U) \subseteq U$. Zeigen Sie:

*a)* Im Falle einer endlichen Untergruppe $U$ ist dann $\varphi(U) = U$.

**Lösung:** Jeder Automorphismus $\varphi$ von $G$ ist insbesondere injektiv; im Falle einer endlichen Untergruppe $U$ hat also $\varphi(U)$ genauso viele Elemente wie $U$. Da $\varphi(U)$ für eine charakteristische Untergruppe $U$ eine Teilmenge von $U$ ist, folgt $\varphi(U) = U$.

*b)* Jede charakteristische Untergruppe $U$ einer Gruppe $G$ ist ein Normalteiler von $G$.

**Lösung:** Für jedes Element $g \in G$ definiert die Konjugation $x \mapsto x^g = g^{-1}xg$ einen Automorphismus von $G$. Im Falle einer charakteristischen Untergruppe $U$ ist also $x^g$ für jedes $x \in U$ wieder ein Element von $U$, und das ist gerade eine der möglichen Charakterisierungen eines Normalteilers.

*c)* Ist $N$ ein Normalteiler der Gruppe $G$ und $U$ eine charakteristische Untergruppe von $N$, so ist $U$ ein Normalteiler der Gruppe $G$.

**Lösung:** Für jedes Element $g \in G$ und jedes $x \in N$ liegt wegen der Normalteilereigenschaft auch $x^g$ in $N$. Die Konjugation mit $g$ ist bildet somit $N$ auf $N$ ab, definiert also einen Automorphismus von $N$. Da $U$ eine charakteristische Untergruppe von $N$ ist, bildet dieser Automorphismus $U$ auf $U$ ab, d.h. für jedes $u \in U$ liegt auch $u^g$ in $U$. Da $g \in G$ beliebig war, folgt die Normalität von $U$ in $G$.

*d)* 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: $[G,G]$ ist eine charakteristische Untergruppe von $G$ !

**Lösung:** Für einen Automorphismus $\varphi$ von $G$ und zwei beliebige Elemente $g, h \in G$ ist

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

das Bild eines Kommutators ist also wieder ein Kommutator und liegt somit in $[G,G]$. Jedes Element von $[G,G]$ läßt sich als Produkt von Kommutatoren schreiben; daher liegt sein Bild unter $\varphi$ als das entsprechende Produkt der Bilder der Kommutatoren auch wieder in $[G,G]$. Somit liegt $\varphi\big([G,G]\big)$ in $[G,G]$, und $[G,G]$ ist eine charakteristische Untergruppe von $G$.

**Aufgabe 3:** *(7 Punkte)*

*a)* Ein Spielzeug-RSA-System arbeitet mit dem Modul $N = 1333 = 31 \cdot 43$. Finden Sie die kleinste natürliche Zahl $e \geq 2$, für die die Abbildung

$$\begin{cases} \mathbb{Z}/N \to \mathbb{Z}/N \\ \quad x \mapsto x^e \end{cases}$$

bijektiv ist!

**Lösung:** Sei $p = 31$ und $q = 43$. Dann ist $p-1 = 30 = 2 \cdot 3 \cdot 5$ und $q = 42 = 2 \cdot 3 \cdot 7$. Die Abbildung $x \mapsto x^e$ ist genau dann bijektiv, wenn $e$ teilerfremd sowohl zu $p-1$ als auch zu $q-1$ ist; $e$ darf also durch keine der vier Primzahlen $2, 3, 5, 7$ teilbar sein. Die kleinste natürliche Zahl $e \geq 2$ mit dieser Eigenschaft ist offensichtlich $e = 11$.

*b)* Bestimmen Sie einen privaten Exponenten $d$ zu dem in *a)* gefundenen öffentlichen Exponenten $e$!

**Lösung:** Das kgV von $p-1$ und $q-1$ ist $2 \cdot 3 \cdot 5 \cdot 7 = 210$. Wir suchen also eine natürliche Zahl $d$ derart, daß $ed = 11d$ modulo 210 gleich eins ist. Der erweiterte EUKLIDische Algorithmus angewendet auf 210 und 11 liefert:

$$210 : 11 = 19 \text{ Rest } 1 \Longrightarrow 1 = 210 - 19 \cdot 11\,;$$

somit ist $-19 \cdot 11 \equiv 1 \bmod 210$. Da wir ein positives $d$ suchen, müssen wir noch 210 addieren und erhalten $d = -19 + 210 = 191$. In der Tat ist $191 \cdot 11 = 2101 \equiv 1 \bmod 210$.

**Aufgabe 4:** (*10 Punkte*)

*a)* Zur Feier des zwanzigsten Jahrestags seines Amtsantritts veranstaltet der Präsident der Unabhängigen Republik Bananien eine große Militärparade. Für die Spitze des Zuges ist eine Musikkapelle vorgesehen. Die Musiker marschieren in sechs Sechserreihen, und in jeder Reihe hat jeder Musiker das gleiche Instrument: Entweder eine Trommel, oder eine Posaune, oder ein Flügelhorn. Alle drei Instrumente sind wirklich vertreten. Eine Trommel wiegt 5 kg, eine Posaune 2 kg und ein Flügelhorn 3 kg. Insgesamt wiegen die Instrumente 108 kg. Wie viele Trommler, Posaunisten und Hornisten nehmen an der Parade teil?

**Lösung:** $x$ sei die Anzahl der Sechserreihen aus Trommlern, $y$ die der Posaunistenreihen und $z$ die der Hornistenreihen. Dann ist $x + y + z = 6$.
Sechs Trommeln wiegen 30 kg, sechs Posaunen 12 kg und sechs Flügelhörner 18 kg. Somit ist $30x + 12y + 18z = 108$. Da alle vorkommenden Zahlen durch sechs teilbar sind, können wir durch sechs dividieren und erhalten das Gleichungssystem

$$x + y + z = 6 \quad \text{und} \quad 5x + 2y + 3z = 18\,.$$

Subtrahieren wir die erste Gleichung zweimal von der zweiten, führt dies auf $3x + z = 6$. Bei diesen kleinen Zahlen brauchen wir keinen Umweg über den erweiterten EUKLIDischen Algorithmus; da $x$ und $z$ beide positiv sein müssen, kommt nur $x = 1$ und $z = 3$ in Frage. Einsetzen in die erste Gleichung zeigt dann, daß $y = 2$ sein muß. Es gibt also sechs Trommler, zwölf Posaunisten und achtzehn Hornisten.

*b)* Dahinter marschiert die Palastwache mit ihren fast Tausend Elitesoldaten. Damit alles einen ordentlichen Eindruck macht, sollen diese in Reihen einer festen Länge marschieren. Bei Zehnerreihen zeigt sich jedoch, daß in der letzten Reihe einer fehlt, um die Reihe voll zu machen, und bei Neunerreihen fehlen sogar zwei. Mit Elferreihen schließlich funktioniert es. Wie viele Soldaten der Palastwache nehmen an der Parade teil?

**Lösung:** $x$ sei die Anzahl der Soldaten. Dann ist

$$x \equiv 9 \bmod 10, \quad x \equiv 7 \bmod 9 \quad \text{und} \quad x \equiv 0 \bmod 11\,.$$

Beginnen wir mit den ersten beiden Kongruenzen. Der ggT von zehn und neun ist natürlich einfach $1 = 10 - 9$, d.h. 10 ist kongruent 0 modulo 10 und 1 modulo 9, und umgekehrt ist -9 kongruent 0 modulo 9 und kongruent 1 modulo 10. Die Zahl $-9 \cdot 9 + 10 \cdot 7 = -11$ ist also kongruent 9 modulo 10 und kongruent 7 modulo 9. Somit ist $x \equiv -11 \bmod 90$; mit positiven Zahlen können wir das auch schreiben als $x \equiv 79 \bmod 90$.
Zusätzlich soll $x \equiv 0 \bmod 11$ sein. Der erweiterte EUKLIDische Algorithmus liefert

$$\begin{aligned} 90 : 11 = 8 \text{ Rest } 2 &\Longrightarrow 2 = 90 - 8 \cdot 11 \\ 11 : 2 = 5 \text{ Rest } 1 &\Longrightarrow 1 = 11 - 5 \cdot 2 = 41 \cdot 11 - 5 \cdot 90 \end{aligned}$$

Also ist $41 \cdot 11 = 451 \equiv 1 \bmod 90$ und $451 \equiv 0 \bmod 11$, und damit ist

$$u = 451 \cdot 79 = 35629 \equiv 79 \bmod 90 \quad \text{und} \quad u \equiv 0 \bmod 11\,.$$

Durch die drei Kongruenzen ist $x$ bestimmt modulo $9 \cdot 10 \cdot 11 = 990$, und $35619 : 990 = 35$ Rest 979. Da $x$ positiv und kleiner 1000 sein muß, kommt nur $x = 979$ in Frage.

**Aufgabe 5:** (*10 Punkte*)

*a)* Wann ist eine Teilmenge I eines (kommutativen) Rings R ein Ideal, und wann ist sie ein Hauptideal?

**Lösung:** I ist genau dann ein Ideal, wenn folgende drei Bedingungen erfüllt sind:

- I ist nicht leer
- Die Summe zweier beliebiger Elemente aus I liegt wieder in I
- Das Produkt eines Elements aus I mit einem beliebigen Element aus R liegt stets in I.

I heißt Hauptideal, wenn es ein $a \in I$ gibt derart, daß $I = (a) = Ra = \{ra \mid r \in R\}$ ist.

*b)* I und J seien Ideale im Ring R. Ist dann auch $I \cup J$ ein Ideal, und ist $I \cap J$ ein Ideal? Beweisen Sie Ihre Aussage oder finden Sie ein Gegenbeispiel!

**Lösung:** $I \cup J$ ist im allgemeinen kein Ideal. Ein Gegenbeispiel im Ring der ganzen Zahlen bilden etwa das Ideal I aller geraden Zahlen und das Ideal J der Dreierzahlen. Zwei und drei liegen beide in $I \cup J$, ihre Summe fünf ist aber weder durch zwei noch durch drei teilbar, liegt also nicht in $I \cup J$.

$I \cap J$ ist stets ein Ideal: Da I und J Ideale sind, sind sie beide nicht leer. Damit enthalten sie auch beide die Null, denn für jedes Element $x$ eines Ideals muß auch $0 \cdot x = 0$ im Ideal liegen. Also ist $0 \in I \cap J$, so daß der Durchschnitt nicht leer ist.

Für zwei Elemente $x, y$ von $I \cap J$ liegen $x$ und $y$ sowohl in I als auch in J; da beides Ideale sind, liegt auch $x + y$ sowohl in I als auch in J, also in $I \cap J$.

Für $x \in I \cap J$ und $r \in R$ schließlich liegt $rx$ sowohl in I als auch in J, also in $I \cap J$.

Damit sind alle drei Idealeigenschaften nachgewiesen.

*c)* Entscheiden Sie, welche der folgenden Teilmengen von $R = \mathbb{Z} \oplus \mathbb{Z}\sqrt{2}$ Ideale sind! Beweisen Sie entweder, daß es sich um ein Ideal handelt, oder zeigen Sie anhand eines Beispiels, daß eine der Forderungen an ein Ideal verletzt ist!

$$I_1 = \{a + b\sqrt{2} \in R \mid a \equiv 0 \bmod 2\}, \qquad I_2 = \{a + b\sqrt{2} \in R \mid b \equiv 0 \bmod 2\},$$
$$I_3 = \{a + b\sqrt{2} \in R \mid a \equiv b \equiv 0 \bmod 2\}, \qquad I_4 = \{a + b\sqrt{2} \in R \mid a + b = 0\},$$
$$I_5 = \{a + b\sqrt{2} \in R \mid a = 0\}, \qquad I_6 = \{a + b\sqrt{2} \in R \mid b = 0\}$$

**Lösung:** Offensichtlich enthalten alle Teilmengen $I_\nu$ die Null, sind also nicht leer, so daß wir diese Bedingung im Folgenden nicht mehr betrachten müssen.

$I_1$ ist ein Ideal, denn sind $a$ und $c$ gerade, so ist auch in $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$ der erste Summand gerade. Weiter ist für $a + b\sqrt{2} \in I_1$ und ein beliebiges $c + d\sqrt{2} \in R$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2},$$

und da $a$ gerade ist, gilt dasselbe für $ac + 2bd$.

$I_2$ ist kein Ideal: Da die Eins in $I_2$ liegt, müßte $I_2$ sonst wegen der dritten Idealeigenschaft ganz R sein, was offensichtlich nicht der Fall ist.

$I_3$ besteht genau aus den Elementen $z = a + b\sqrt{2}$ von R, für die es Elemente $w = c + d\sqrt{2}$ in R gibt, für die $z = 2w$ ist. Somit ist $I_3$ das von der Zwei erzeugte Hauptideal von R.

$I_4$ besteht genau aus den Elementen der Form $a - a\sqrt{2} = a(1 - \sqrt{2})$ mit $a \in \mathbb{Z}$. Dies ist kein Ideal, denn zwar liegt $1 - \sqrt{2}$ in $I_4$, das Produkt $\sqrt{2} \cdot (1 - \sqrt{2}) = -2 + \sqrt{2}$ aber nicht.

$I_5 = \mathbb{Z}\sqrt{2}$ ist ebenfalls kein Ideal: $\sqrt{2} \in I_5$, aber $\sqrt{2} \cdot \sqrt{2} = 2 \notin I_5$.

Entsprechend ist auch $I_6 = \mathbb{Z}$ kein Ideal, denn $1 \in I_6$, aber $I_6 \neq R$.

*d)* Zeigen Sie, daß die Ideale unter diesen Mengen allesamt Hauptideale sind! Erraten Sie dazu ein möglichst einfaches Element der Menge, von dem Sie zeigen können, daß alle anderen Vielfache davon sind!

**Lösung:** $I_3$ ist, wie wir gesehen haben, das von der Zwei erzeugte Hauptideal.

Das zweite Ideal unter den sechs Teilmengen ist $I_1$. Eines der einfachsten Elemente von $I_1$ ist die Zwei, aber offensichtlich ist $I_1 \neq (2)$. Auch $\sqrt{2}$ liegt in $I_1$, und damit haben wir Erfolg: Für jedes Element $x \in I_1$ gibt es $b, c \in \mathbb{Z}$, so daß

$$x = 2c + b\sqrt{2} = \left(b + c\sqrt{2}\right) \cdot \sqrt{2}$$

ist, d.h. $I_1$ ist das von $\sqrt{2}$ erzeugte Hauptideal.

**Aufgabe 6:** (*8 Punkte*)

*a)* Bestimmen Sie den Inhalt $I(f)$ sowie den primitiven Anteil $f^*$ für das Polynom $f = 3X^5 - 6X^4 + 9X^3 - 12X^2 + 6X \in \mathbb{Z}[X]$!

**Lösung:** Alle Koeffizienten sind durch drei teilbar, und da die Drei selbst als Koeffizient vorkommt, ist der Inhalt $I(f)$ als ggT aller Koeffizienten gleich drei. Der primitive Anteil ist somit $f^* = X^5 - 2X^4 + 3X^3 - 4X^2 + 2X$.

*b)* Die Eins ist eine mehrfache Nullstelle von $f$ und damit auch von $f^*$. Bestimmen Sie ihre Vielfachheit!

**Lösung:** In der Tat ist $f^*(1) = 1 - 2 + 3 - 4 + 2 = 0$. Die Vielfachheit dieser Nullstelle könnten wir über die Ableitungen von $f^*$ berechnen; da $f$ aber in *c)* noch faktorisiert werden soll, können wir auch gleich $X - 1$ so lange wie möglich abdividieren:

$$(X^5 - 2X^4 + 3X^3 - 4X^2 + 2X) : (X - 1) = X^4 - X^3 + 2X^2 - 2X$$
$$(X^4 - X^3 + 2X^2 - 2X) : (X - 1) = X^3 + 2X = X(X^2 + 2)$$

Der letzte Quotient ist offensichtlich nicht mehr durch $X - 1$ teilbar; daher ist die Eins eine doppelte Nullstelle von $f^*$ und damit auch von $f$.

*c)* Zerlegen Sie $f$ sowohl in $\mathbb{Q}[X]$ als auch in $\mathbb{Z}[X]$ in seine irreduziblen Faktoren! Wie viele verschiedene irreduzible Faktoren gibt es jeweils?

**Lösung:** Wie wir gerade gesehen haben, ist $f^* = (X - 1)^2X(X^2 + 2)$ und damit ist $f = 3(X - 1)^2X(X^2 + 2)$. Die Polynome $X - 1$, $X$ und $X^2 + 2$ sind in $\mathbb{Q}[X]$ irreduzibel: Bei den linearen Polynomen ist das offensichtlich, und $X^2 + 2$ müßte im Falle der Reduzibilität eine rationale Nullstelle haben, hat aber nicht einmal eine reelle. Da alle Polynome primitiv sind, sind sie auch in $\mathbb{Z}[X]$ irreduzibel. Der Vorfaktor drei ist in $\mathbb{Q}[X]$ eine Einheit, in $\mathbb{Z}[X]$ aber als Primzahl ein irreduzibles Element. In $\mathbb{Q}[X]$ gibt es somit drei verschiedene irreduzible Faktoren, in $\mathbb{Z}[X]$ vier.

*d)* Finden Sie einen endlichen Erweiterungskörper $K/\mathbb{Q}$ mit der Eigenschaft, daß $f$ über $K$ in Linearfaktoren zerfällt!

**Lösung:** Nur der Faktor $X^2 + 2$ kann noch weiter zerlegt werden: Über $K = \mathbb{Q}(\sqrt{-2})$ ist $X^2 + 2 = (X + \sqrt{-2})(X - \sqrt{-2})$, und damit ist in $K[X]$

$$f = 3 \cdot (X - 1)^2 \cdot X \cdot (X + \sqrt{-2}) \cdot (X - \sqrt{-2}),$$

wobei die Drei natürlich auch in $K$ und in $K[X]$ eine Einheit ist.

*e)* Welchen Grad hat der Zerfällungskörper von $f$ über $\mathbb{Q}$?

**Lösung:** $[K : \mathbb{Q}] = 2$, und da $f$ in $\mathbb{Q}[X]$ nicht in Linearfaktoren zerfällt, kann es keinen kleineren Körper geben, über dem $f$ zerfällt. $K$ ist somit Zerfällungskörper, und der gesuchte Grad ist zwei.

**Aufgabe 7:** (*12 Punkte*)

*a)* Zeigen Sie, daß $\mathbb{Q}(\sqrt{12}, \sqrt{24})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ und $\mathbb{Q}(\sqrt{3} - \sqrt{2})$ denselben Teilkörper $K$ von $\mathbb{R}$ definieren!

**Lösung:** Da $\sqrt{12} = 2\sqrt{3}$ und $\sqrt{24} = 2\sqrt{2}\sqrt{3}$ ist, liegen $\sqrt{12}$ und $\sqrt{24}$ in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$; genauso liegen auch $\sqrt{2} = \sqrt{24}/\sqrt{12}$ und $\sqrt{3} = \frac{1}{2}\sqrt{12}$ in $\mathbb{Q}(\sqrt{12}, \sqrt{24})$. Somit stimmen die Körper $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ und $\mathbb{Q}(\sqrt{12}, \sqrt{24})$ überein.
$k = \mathbb{Q}(\sqrt{3} - \sqrt{2})$ liegt natürlich in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Als Körper enthält $k$ auch das Quadrat $(\sqrt{3} - \sqrt{2})^2 = 5 - 2\sqrt{6}$, also auch $\sqrt{6}$ und $\sqrt{6} \cdot (\sqrt{3} - \sqrt{2}) = 3\sqrt{2} - 2\sqrt{3}$. Damit liegt auch $(3\sqrt{2} - 2\sqrt{3}) + 2(\sqrt{3} - \sqrt{2}) = \sqrt{2}$ in $k$, also auch $\sqrt{3} = (\sqrt{3} - \sqrt{2}) + \sqrt{2}$. Somit ist $k = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

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

**Lösung:** $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$ enthält den Körper $\mathbb{Q}(\sqrt{2})$; als Vektorraum über $\mathbb{Q}(\sqrt{2})$ ist $K = \mathbb{Q}(\sqrt{2}) \oplus \mathbb{Q}(\sqrt{2})\sqrt{3}$. Da $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2}$ ist, folgt $K = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}\sqrt{3} \oplus \mathbb{Q}\sqrt{6}$. Damit ist $[K : \mathbb{Q}] = 4$.

*c)* Zeigen Sie, daß $K/\mathbb{Q}$ Galoissch ist, und bestimmen Sie $\mathrm{Aut}(K/\mathbb{Q})$!

**Lösung:** Ein Automorphismus $\varphi \in \mathrm{Aut}(K/\mathbb{Q})$ muß $\mathbb{Q}$ fest lassen, ist also eindeutig bestimmt durch die Bilder der Basiselemente. Natürlich muß $\varphi(1) = 1$ sein. Da $\left(\sqrt{2}\right)^2 = 2$ ist, muß auch $\varphi\left(\sqrt{2}\right)^2 = \varphi(2) = 2$ sein, d.h. $\varphi\left(\sqrt{2}\right) = \pm\sqrt{2}$. Ein analoges Argument zeigt, daß $\varphi\left(\sqrt{3}\right) = \pm\sqrt{3}$ sein muß. Das noch fehlende Bild $\varphi\left(\sqrt{6}\right) = \varphi\left(\sqrt{2}\right) \cdot \varphi\left(\sqrt{3}\right)$ ist durch die Bilder von $\sqrt{2}$ und $\sqrt{3}$ festgelegt. Also haben wir vier Automorphismen; abgesehen von der Identität sind dies die Abbildungen $\rho, \sigma, \tau$ mit $\rho\left(\sqrt{2}\right) = -\sqrt{2}$ und $\rho\left(\sqrt{3}\right) = \sqrt{3}$, $\sigma\left(\sqrt{2}\right) = \sqrt{2}$ und $\sigma\left(\sqrt{3}\right) = -\sqrt{3}$, $\tau\left(\sqrt{2}\right) = -\sqrt{2}$ und $\tau\left(\sqrt{3}\right) = -\sqrt{3}$. Die Erweiterung $K/\mathbb{Q}$ ist Galoissch, denn ist $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ ein Element des Fixkörpers von $\mathrm{Aut}(K/\mathbb{Q})$, ist $\rho(x) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} = x$, also ist wegen der Eindeutigkeit der Basisdarstellung $b = d = 0$. Genauso folgt aus $\sigma(x) = x$, daß $c = 0$ sein muß. Daher liegt $x = a \in \mathbb{Q}$, der Fixkörper ist also $\mathbb{Q}$.

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

**Lösung:** Die Galois-Gruppe hat vier Elemente; abgesehen von der Identität erzeugt jedes eine Untergruppe der Ordnung zwei. Die Zwischenkörper sind daher

$$K^{<\rho>} = \mathbb{Q}(\sqrt{3}), \qquad K^{<\sigma>} = \mathbb{Q}(\sqrt{2}) \quad \text{und} \quad K^{<\tau>} = \mathbb{Q}(\sqrt{6}),$$

wobei $\langle g\rangle$ 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 $\left(\sqrt{3} - \sqrt{2}\right)^2 = 5 - 2\sqrt{6}$ ist. Für $x = \sqrt{3} - \sqrt{2}$ ist also $(x^2 - 5)^2 = 4 \cdot 6 = 24$, d.h. $f = (X^2 - 5)^2 - 24 = X^4 - 10X^2 + 1$ hat $\sqrt{3} - \sqrt{2}$ als Nullstelle. Da $f$ rationale Koeffizienten hat, muß $f$ auch die Bilder von $\sqrt{3} - \sqrt{2}$ unter den Automorphismen von $K/\mathbb{Q}$ als Nullstellen haben, d.h. $f$ verschwindet für jede der vier Zahlen $\pm\sqrt{2} \pm \sqrt{3}$. Wäre $f$ nicht irreduzibel in $\mathbb{Q}[X]$, gäbe es ein Polynom $g \in \mathbb{Q}[X]$ vom Grad kleiner vier, das an der Stelle $\sqrt{3} - \sqrt{2}$ verschwände, und auch $g$ müßte alle vier Bilder als Nullstellen haben. Das ist für ein Polynom vom Grad kleiner vier nicht möglich; somit ist $f$ irreduzibel. 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 $\mathbb{Q}\left(\sqrt{2}\right)$ in seine irreduziblen Faktoren!

**Lösung:** $\mathbb{Q}\left(\sqrt{2}\right)$ ist der Fixkörper von $\sigma$; ein Faktor, der $\sqrt{3} - \sqrt{2}$ als Nullstelle hat, muß daher auch $\sigma\left(\sqrt{3} - \sqrt{2}\right) = -\sqrt{2} - \sqrt{3}$ als Nullstelle haben.

$$g = \left(X + \sqrt{2} + \sqrt{3}\right)\left(X + \sqrt{2} - \sqrt{3}\right) = \left(X + \sqrt{2}\right)^2 - 3 = X^2 + 2\sqrt{2}X - 1$$

ist ein Polynom aus $\mathbb{Q}\left(\sqrt{2}\right)[X]$ mit diesen beiden Nullstellen. Das Polynom

$$h = \left(X - \sqrt{2} + \sqrt{3}\right)\left(X - \sqrt{2} - \sqrt{3}\right) = \left(X - \sqrt{2}\right)^2 - 3 = X^2 - 2\sqrt{2} - 1$$

liegt ebenfalls dort und verschwindet bei den beiden übrigen Nullstellen von $f$. Somit ist

$$f = \left(X + \sqrt{2} + \sqrt{3}\right)\left(X - \sqrt{2} + \sqrt{3}\right)\left(X + \sqrt{2} - \sqrt{3}\right)\left(X - \sqrt{2} - \sqrt{3}\right) = gh,$$

und $g, h$ sind irreduzibel über $\mathbb{Q}\left(\sqrt{2}\right)$, da jedes Polynom über diesem Körper mit einem Element aus $K$ auch dessen Bild unter $\sigma$ als Nullstelle haben muß.