Übungsblatt 12: Abschluss

1. Primitive Elemente

V 1.1. (a) Sei $E|K$ eine endliche Galoiserweiterung. Zeigen Sie (mit Hilfe der Galoiskorrespondenz), dass für $\alpha \in E$ die beiden Aussagen äquivalent sind:
(i) Für alle $\sigma \in \mathrm{Aut}(E|K)\backslash\{\mathrm{id}\}$ gilt $\sigma(\alpha) \neq \alpha$.
(ii) Es gilt $E = K[\alpha]$, d.h. α ist ein primitives Element.
(b) Zeigen Sie $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ direkt durch Mengeninklusionen.
(c) Zeigen Sie $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ mit Hilfe von Teil (a).

Lösungshinweise: —

(a) *Der Körper $K[\alpha]$ ist ein Zwischenkörper der Galoiserweiterung $E|K$ und entspricht somit einer Untergruppe der Galoisgruppe $\mathrm{Aut}(E|K)$, die diesen Körper als Fixkörper besitzt. Nun besagt die erste Aussage, dass kein nichttrivialer Automorphismus α festhält und somit besteht die zugehörige Untergruppe nur aus der Identität. Dies ist aber wiederrum nach Galois äquivalent dazu, dass $K[\alpha] = E$.*

(b) $\mathbb{Q}[\sqrt{2},\sqrt{3}] \supset \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ *ist klar. Aus* $\sqrt{2} = \frac{1}{2}\left((\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})\right) \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ *und damit* $\sqrt{3} = (\sqrt{2}+\sqrt{3}) - \sqrt{2} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ *folgt auch* $\mathbb{Q}[\sqrt{2},\sqrt{3}] \subset \mathbb{Q}[\sqrt{2}+\sqrt{3}]$.

(c) *Nach Aufgabe 4.6 von Blatt 10 sind die Bilder von* $\alpha = \sqrt{2}+\sqrt{3}$ *unter den nichttrivialen Automorphismen von* $\mathbb{Q}[\sqrt{2},\sqrt{3}]|\mathbb{Q}$ *gerade* $-\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$ *und* $-\sqrt{2}-\sqrt{3}$. *Diese sind alle von* α *verschieden und damit ist* $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ *nach Teil (a).*

—

1.2. Finden Sie ein primitives Element der Erweiterung $\mathbb{Q}[i,\sqrt[4]{2}]$ über $\mathbb{Q}$.

Lösungshinweise: — *Betrachte* $\alpha = i+\sqrt[4]{2}$ *unter den Automorphismen aus Aufgabe 1.1 von Blatt 11. Es ergeben sich die Bilder* $i+i\sqrt[4]{2}$, $i-\sqrt[4]{2}$, $i-i\sqrt[4]{2}$, $-i+\sqrt[4]{2}$, $-i+i\sqrt[4]{2}$, $-i-\sqrt[4]{2}$ *und* $-i-i\sqrt[4]{2}$, *die alle von* α *verschieden sind. Damit ist* $i+\sqrt[4]{2}$ *nach Aufgabe 1.1 (a) (von diesem Blatt) ein primitives Element.*
—

1.3. Bestimmen Sie alle primitiven Elemente von $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ über $\mathbb{Q}$.

Lösungshinweise: — *Ein allgemeines Element in* $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ *hat die Form* $\alpha = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ *mit* $a,b,c,d \in \mathbb{Q}$. *Die Bilder unter den nichttrivialen Automorphismen von* $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ *über* $\mathbb{Q}$ *sind gegeben durch* $a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$, $a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$ *und* $a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$. *Damit diese alle von* α *verschieden sind, müssen mindestens zwei der drei Koeffizienten* b,c,d *von Null verschieden sein und dies legt nach Aufgabe 1.1 (a) alle primitiven Elemente fest* —

2. Spezielle Erweiterungen

2.1. Sei $E|K$ eine galoissche Körpererweiterung. Wir nennen $E|K$ abelsch, bzw. zyklisch, wenn die Galoisgruppe $\mathrm{Aut}(E|K)$ abelsch bzw. zyklisch ist.
(a) Es sei $E|K$ eine abelsche Galoiserweiterung. Zeige, dass dann für jeden Zwischenkörper F auch $E|F$ und $F|K$ abelsche Galoiserweiterungen sind.
(b) Es sei $E|K$ eine zyklische Galoiserweiterung. Zeige, dass dann für jeden Zwischenkörper F auch $E|F$ und $F|K$ zyklische Galoiserweiterungen sind.

Lösungshinweise: — *Untergruppen und Quotientengruppen abelscher und zyklischer Gruppen sind wieder abelsch bzw. zyklisch. Weiter ist jede Untergruppe einer abelschen (zyklischen) Gruppe normal. Damit folgen die Aussagen direkt aus der Galoiskorrespondenz.* —

2.2. Zeigen Sie, dass jede Körpererweiterung vom Grad 2 normal ist.

Lösungshinweise: — *Sei $|E:K|=2$. Dann wissen wir, dass $E=K[u]$ gilt und u ist Nullstelle eines quadratischen Polynoms $P=x^2+ax+b=(x-u)(x-v)$. Wir müssen zeigen, dass $v\in K[u]$ liegt. Es gilt aber $a=-u-v$ und somit $v=-a-u\in K[u]$, wie gewünscht. Damit ist E Zerfällungskörper des Polynoms P und somit normal.*
Man vergleiche diese Aussage mit der Aussage der Gruppentheorie, dass jede Untergruppe vom Index 2 normal ist. —

2.3. Welche der folgenden Erweiterungen sind normal?
(a) $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ über $\mathbb{Q}$
(b) $\mathbb{Q}[e^{2\pi i/n}]$ über $\mathbb{Q}$
(c) $\mathbb{Q}[\sqrt[4]{2}]$ über $\mathbb{Q}$
(d) $\mathbb{Q}[i][\sqrt[4]{2}]$ über $\mathbb{Q}[i]$

Lösungshinweise: —
(a) *Zerfällungskörper des Polynom $(X^2-2)(X^2-3)$, also normal.*
(b) *Zerfällungskörper des Polynom X^n-1, also normal.*
(c) *Nicht normal, da das Polynom X^4-2 die Nullstellen $\pm\sqrt[4]{2}$ in $\mathbb{Q}[\sqrt[4]{2}]$ besitzt, aber die Nullstellen $\pm i\sqrt[4]{2}$ nicht in $\mathbb{Q}[\sqrt[4]{2}]$ enthalten sind.*
(d) *Normal, da Zerfällungskörper des Polynoms X^4-2. Die Multiplikation mit i liefert nun auch die beiden anderen Nullstellen.*

—

2.4. Sei E eine endliche algebraische Körpererweiterung von K, sodass die Charakteristik p von K den Grad der Körpererweiterung $|E:K|$ nicht teilt. Zeigen Sie, dass die Körpererweiterung separabel ist.
Hinweis: Ein irreduzibles Polynom P ist genau dann separabel, wenn $P'\neq 0$.

Lösungshinweise: — *Sei $a\in E$ ein Element mit Minimalpolynom $P=X^n+Q$ und $\deg(Q)<n$. Dann ist nach Gradformel $n=|K[a]:K|$ ein Teiler von $|E:K|$ und somit ist n teilerfremd zu p. Es folgt $P'=nX^{n-1}+Q'\neq 0$ und damit ist P und also auch a separabel. Damit sind alle Elemente aus E separabel, was zu zeigen war.* —

3. Inverses Galoisproblem

V 3.1. Der Satz von Dirichlet aus der Zahlentheorie liefert für gegebenes $a\in\mathbb{N}$ unendlich viele Primzahlen der Form $p=1+ka$.
(a) Zeigen Sie unter Benutzung dieses Resultats, dass jede endliche zyklische Gruppe $\mathbb{Z}/a$ zu einer Quotientengruppe von $\mathbb{Z}/p^\times$ isomorph ist.
(b) Folgern Sie aus dem chinesischen Restsatz, dass dies auch für jede endliche abelsche Gruppe gilt, wenn wir $\mathbb{Z}/n^\times$ für geeignetes $n\in\mathbb{N}$ betrachten.
(c) Benutzen Sie nun die Aussage $\mathrm{Aut}(\mathbb{Q}[e^{2\pi i/n}]|\,\mathbb{Q})\cong\mathbb{Z}/n^\times$, um zu zeigen, dass sich jede endliche abelsche Gruppe als Galoisgruppe über $\mathbb{Q}$ realisieren lässt.

Lösungshinweise: —
(a) *Sei $a\in\mathbb{N}$ gegeben. Dann gibt es eine Primzahl p mit $p=1+ka$ für ein $k\in\mathbb{N}$. Damit ist dann die Gruppe $\mathbb{Z}/p^\times$ nach Vorlesung zyklisch und hat ka Elemente, ist also isomorph zu $\mathbb{Z}/ka$. Darin gibt es die Untergruppe (den Normalteiler) $a\mathbb{Z}/ka$ und nach dem dritten Isomorphiesatz (9B15) ist $(\mathbb{Z}/ka)/(a\mathbb{Z}/ka)\cong\mathbb{Z}/a$. Damit ist $\mathbb{Z}/a$ isomorph zu einem Quotienten von $\mathbb{Z}/p^\times$.*

(b) *Eine endliche abelsche Gruppe A ist nach dem Klassifikationssatz isomorph zu einem direkten Produkt zyklischer Gruppen* $\mathbb{Z}/_{q_1^{l_1}} \times \cdots \times \mathbb{Z}/_{q_k^{l_k}}$ *mit Primzahlen* $q_i \in \mathbb{N}$. *Wir wählen wie in (a) k verschiedene Primzahlen* $p_1, \ldots, p_k$, *so dass* $\mathbb{Z}/_{q_i^{l_i}}$ *als Quotient von* $\mathbb{Z}/_{p_i}^{\times}$ *realisiert werden kann. Damit ist dann A isomorph zu einem Quotient der Gruppe* $\mathbb{Z}/_{p_1}^{\times} \times \cdots \times \mathbb{Z}/_{p_k}^{\times}$. *(Man beachte:* $(G_1 \times \cdots \times G_k)/(H_1 \times \cdots \times H_k) \cong G_1/H_1 \times \cdots \times G_k/H_k$.*) Nach chinesischem Restsatz gilt* $\mathbb{Z}/_{p_1 \cdots p_k}^{\times} \cong \mathbb{Z}/_{p_1}^{\times} \times \cdots \times \mathbb{Z}/_{p_k}^{\times}$ *für verschiedene Primzahlen* $p_1, \ldots, p_k$ *(da diese teilerfremd sind) und somit ist A isomorph zu einem Quotienten von* $\mathbb{Z}/_{p_1 \cdots p_k}^{\times}$.

(c) *Da jede abelsche Gruppe A als Quotient* $(\mathbb{Z}/_n^{\times})/N$ *realisiert werden kann, wenn n passend gewählt ist, finden wir unsere gewünschte Erweiterung mit Galoisgruppe A, indem wir zuerst* $\mathbb{Q}[e^{2\pi i/n}]|\,\mathbb{Q}$ *betrachten. Diese hat als Automorphismengruppe* $G = \mathrm{Aut}(\mathbb{Q}[e^{2\pi i/n}]|\,\mathbb{Q}) \cong \mathbb{Z}/_n^{\times}$. *Darin gibt es nach Galoiskorrespondenz einen zum Normalteiler N gehörigen Zwischenkörper F, so dass* $F|\mathbb{Q}$ *galoissch ist und eine zu* $G/N \cong A$ *isomorphe Galoisgruppe besitzt.*

—

4. Symmetrische Polynome

4.1. Ein Polynom $s \in K[X_1, \ldots, X_n]$ heißt symmetrisch in den Variablen $X_1, \ldots, X_n$, wenn $s(X_1, \ldots, X_n) = s(X_{\pi(1)}, \ldots, X_{\pi(n)})$ für alle $\pi \in S_n$.

(a) Sei $P(X) = X^n + s_1 X^{n-1} + \ldots + s_n = (X + X_1)(X + X_2) \cdots (X + X_n)$. Man nennt s_i das *elementarsymmetrische Polynom* vom Grad i in $X_1, \ldots, X_n$. Man schreibe diese möglichst explizit hin.

(b) Zeigen Sie, dass sich für $n = 2$ jedes symmetrische Polynom $s(X_1, X_2)$ als Polynom in s_1 und s_2 schreiben lässt. Können Sie diese Aussage auf $n > 2$ verallgemeinern?

(c) Zeigen Sie, dass die *Diskriminante* $D_n := \prod_{i<j} (X_i - X_j)^2$ von P in $K[X_1, \ldots, X_n]$ symmetrisch ist und stellen Sie D_2 als Polynom in s_1 und s_2 dar. Welcher Zusammenhang besteht zur Mitternachtsformel?

Lösungshinweise: —

(a) *Vertauscht man die Faktoren auf der rechten Seite der Gleichung* $X^n + s_1 X^{n-1} + \ldots + s_n = (X - X_1)(X - X_2) \cdots (X - X_n)$, *so ändert sich wegen der Kommutativität der Multiplikation nichts an den Koeffizienten links. Damit müssen diese symmetrisch in* $X_1, \ldots, X_n$ *sein.*
Für $n = 3$ *ergeben sich z.B.* $s_1 = X_1 + X_2 + X_3, s_2 = X_1X_2 + X_1X_3 + X_2X_3$ *und* $s_3 = X_1X_2X_3$. *Allgemein kann man das (z.B.) in der Form* $s_i = \sum_{\substack{S \subset \{1,\ldots,n\} \\ |S| = k}} \prod_{i \in S} X_i$ *schreiben.*

(b) *Es gilt* $s_1 = X_1 + X_2$ *und* $s_2 = X_1X_2$. *Ein allgemeines symmetrisches Polynom* $P(X_1, X_2)$ *in zwei Variablen ist entweder null oder enthält einen Term, in dem* X_1 *mit der höchsten Potenz auftritt. Also* $P(X_1, X_2) = aX_1^n X_2^k + R(X_1, X_2)$. *Es muss* $n \geq k$ *gelten, da sonst wegen Symmetrie der Term* $aX_1^k X_2^n$ *in P auftreten würde und eine höhere* X_1*-Potenz enthielte. Falls* $n = k$, *so lässt sich der Term* $aX_1^n X_2^n = as_2^n$ *durch* s_2 *ausdrücken. Falls* $n > k$, *betrachte man* $aX_1^n X_2^k - as_1^{n-k} s_2^k$. *Dieser enthält* X_1 *nur noch zur Potenz* $n - 1$.
Wenn wir nun alle Terme, in denen X_1^n *auftritt, so umformen, so können wir* $P(X_1, X_2)$ *als Summe eines Polynoms in* s_1 *und* s_2 *und eines neuen Polynoms* P_1 *schreiben, dass* X_1 *höchstens noch zur* $(n-1)$*-ten Potenz enthält. Der Rest ist Induktion.*
Die allgemeine Aussage für $n \in \mathbb{N}$ *ist der* Hauptsatz über symmetrische Polynome. *Falls Sie an einem Beweis interessiert sind, lesen Sie diesen in einem geeigneten Buch oder Skript nach. Der Beweis ist nicht schwieriger als im Fall* $n = 2$, *benötigt aber etwas mehr Notation.*

(c) *Die symmetrische Gruppe S_n operiert auf Paaren (i,j) mit $1 \leq i < j \leq n$ folgendermaßen. Falls $\pi(i) < \pi(j)$, wird (i,j) auf $(\pi(i),\pi(j))$ abgebildet, sonst auf $(\pi(j),\pi(i))$. Wegen $(X_i - X_j)^2 = (X_j - X_i)^2$ operiert S_n also auch auf den Faktoren dieses Produktes und wegen der Kommutativität der Multiplikation ist D_n symmetrisch in $X_1,\dots,X_n$.*
Es ist $(X_1 - X_2)^2 = (X_1 + X_2)^2 - 4X_1X_2 = s_1^2 - 4s_2$. Für ein Polynom $X^2 + bX + c$ ist die Diskriminante also gerade der Term $b^2 - 4c$ unter der Wurzel in der Mitternachtsformel.

—

5. Lösen polynomieller Gleichungen durch Radikale

5.1. Wir wollen hier eine Formel für die Nullstellen einer allgemeinen kubischen Gleichung über $\mathbb{C}$ bestimmen.

(a) Führen Sie zuerst die Gleichung $ax^3 + bx^2 + cx + d = 0$ mit $a \neq 0$ durch eine Transformation der Form $x \mapsto z + h$ in $z^3 + pz + q = 0$ über.

(b) Führen Sie die Substitution $z = u + v$ durch und folgern Sie, dass $p = -3uv$ und $q = -(u^3 + v^3)$ gilt.

(c) Stellen Sie eine quadratische Gleichung auf, die als Lösungen u^3 und v^3 besitzt und drücken Sie die Koeffizienten durch p und q aus. Wir erhalten

$$u^3 = -\frac{q}{2} + \sqrt{D} \text{ und } v^3 = -\frac{q}{2} - \sqrt{D} \text{ mit } D := \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3.$$

(d) Zeigen Sie, dass $u+v, ju+j^2v, j^2u+jv$ mit $j = e^{2\pi i/3}$ dann alle Lösungen der obigen Gleichung $z^3 + pz + q = 0$ sind, wenn man für u und v zwei dritte Wurzeln wählt, die der Bedingung $p = -3uv$ genügen.

(e) Bestimmen Sie die Lösungen der Gleichung $x^3 + 3x^2 + 6x + 6 = 0$.

Lösungshinweise: —

(a) *Teilen der Gleichung durch a und anschließende Translation um $h = -\frac{b}{3a}$ liefert $p = -\frac{b^2}{3a^2} + \frac{c}{a}$ und $q = \frac{2b^3}{3^3a^3} - \frac{cb}{3a} + \frac{d}{a}$.*

(b) *Es ist $z^3 = (u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = 3uv(u+v) + u^3 + v^3 = -pz + -q$. Ein Koeffizientenvergleich liefert $p = -3uv$ und $q = -(u^3 + v^3)$.*

(c) *Offenbar hat $(X - u^3)(X - v^3) = X^2 - (u^3 + v^3)X + u^3v^3 = X^2 + qX - \left(\frac{p}{3}\right)^3$ die Nullstellen u^3 und v^3, aber nach Mitternachtsformel sind diese auch gleich $-\frac{q}{2} \pm \sqrt{D}$, wie man leicht nachrechnet.*

(d) *Man multipliziere das Polynom $(z - (u+v))(z - (ju + j^2v))(z - (j^2u + jv))$ aus und verwende die Beziehungen $1 + j + j^2 = 0$, $-3uv = p$ und $-u^3 - v^3 = q$ und man erhält das ursprüngliche Polynom $z^3 + pz + q$ zurück. Also sind die drei Zahlen wirklich die gesuchten Nullstellen.*

(e) *Die lineare Transformation mit $h = -1$ führt auf das Polynom $z^3 + 3z + 2$, also $p = 3, q = 2$. Es ist also $D = 2$ und somit $u^3 = -1 + \sqrt{2}$ und $v^3 = -1 - \sqrt{2}$. Wählt man für u und v die beiden reellen dritten Wurzeln, so erfüllen sie die geforderte Bedingung an p und wir erhalten $u = \sqrt[3]{-1 + \sqrt{2}}$ und $v = -\sqrt[3]{1 + \sqrt{2}}$. Die Lösungen der Gleichung ist also gegeben durch*
$z_1 = u + v + h = \sqrt[3]{-1 + \sqrt{2}} - \sqrt[3]{1 + \sqrt{2}} - 1$
$z_2 = ju + j^2v + h = \frac{-1+\sqrt{3}i}{2}\sqrt[3]{-1 + \sqrt{2}} - \frac{-1-\sqrt{3}i}{2}\sqrt[3]{1 + \sqrt{2}} - 1$
$z_3 = j^2u + jv + h = \frac{-1+\sqrt{3}i}{2}\sqrt[3]{-1 + \sqrt{2}} - \frac{-1+\sqrt{3}i}{2}\sqrt[3]{1 + \sqrt{2}} - 1.$

—

5.2. Sind die folgenden Gleichungen durch Radikale lösbar?

(a) $x^5 - 9x + 3 = 0$

(b) $x^6 + 12x^4 - 9x^2 - 3 = 0$

(c) $x^{11} = 17$

Lösungshinweise: —

(a) *Das Polynom $P(x) = x^5 - 9x + 3$ ist nach Eisenstein zu $p = 3$ irreduzibel und hat genau 3 reelle Nullstellen. Denn die Ableitung $P'(x) = 5x^4 - 9$ hat offenbar genau zwei reelle Nullstellen und nach dem Satz von Rolle (Analysis 1) kann P höchstens drei Nullstellen besitzen. (Eine mehrfache Nullstelle gibt es auch nicht, weil $ggT(P,P') = 1$ ist.) Wegen $f(-2) = -14 < 0$, $f(0) = 3 > 0$, $f(1) = -5 < 0$ und $f(2) = 20 > 0$, muss es nach Zwischenwertsatz aber mindestens drei Nullstellen geben.*
Nach dem Fundamentalsatz der Algebra hat also P zwei komplexe Nullstellen und weil die Koeffizienten von P reell sind, sind die beiden komplex konjugiert. Der Zerfällungskörper E des Polynoms enthält also die komplexe Konjugation als Automorphismus. Andererseits muss der Grad der Körpererweiterung $|E : \mathbb{Q}|$ durch den Grad des (irreduziblen!) Polynoms P teilbar sein, also teilt 5 die Gruppenordnung der Galoisgruppe G und somit enthält G nach dem Satz von Cauchy (oder Sylow) ein Element der Ordnung 5.
Andererseits permutiert die Galoisgruppe die Nullstellen von P und ist damit isomorph zu eines Untergruppe der S_5. Nach Aufgabe 1.3 von Blatt 8 muss G sogar zu ganz S_5 isomorph sein.
Da $A_5 < S_5$ nicht auflösbar ist, folgt aus dem Auflösbarkeitsresultat der Vorlesung, dass die Gleichung $x^5 - 9x + 3 = 0$ nicht durch Radikale auflösbar ist.

(b) *Man kann das Polynom $x^6 + 12x^4 - 9x^2 - 3$ als ein kubisches Polynom in der Variablen $y = x^2$ schreiben. Da jede Gleichung vom Grad ≤ 4 auflösbar ist, kann man die Lösungen y_1, y_2, y_3 mit Hilfe von zweiten und dritten Wurzeln darstellen und danach kann man die 6 Lösungen durch erneutes Quadratwurzelziehen aus den y_i gewinnen. Insgesamt erhält man für die Lösungen eine Darstellung durch Radikale.*

(c) *Das Polynom ist nach Definition durch Radikale auflösbar.*

—

6. SONSTIGES

6.1. Sei $E|K$ eine Galoiserweiterung und $a \in E$. Zeigen Sie, dass

$$\text{die Spur } tr(a) := \sum_{\sigma \in \mathrm{Aut}(E|K)} \sigma(a) \quad \text{und die Norm } N(a) := \prod_{\sigma \in \mathrm{Aut}(E|K)} \sigma(a)$$

Elemente aus K sind.

Lösungshinweise: — *Für einen Automorphismus $\tau \in \mathrm{Aut}(E|K)$ gilt $\tau(tr(a)) = \tau\left(\sum_{\sigma \in \mathrm{Aut}(E|K)} \sigma(a)\right) = \sum_{\sigma \in \mathrm{Aut}(E|K)} \tau(\sigma(a)) = \sum_{\sigma \in \mathrm{Aut}(E|K)} \sigma(a) = tr(a)$, da die Linksmultiplikation in einer Gruppe bijektiv ist. Dies funktioniert ebenso für die Norm, weil Automorphismen multiplikativ sind. Die einzigen Elemente, die immer unter der Operation der Galoisgruppe festbleiben sind die Elemente in K, was zu zeigen war.* —

6.2. Ein berühmter Satz von Lindemann besagt, dass für $a \in \mathbb{C}$ algebraisch, die Zahl e^a transzendent ist. Man folgere daraus, dass π transzendent ist.

Lösungshinweise: — *Es ist $e^{2\pi i} = 1$ algebraisch und somit kann der Exponent $2\pi i$ nach Lindemann nicht algebraisch sein. Da 2 und i algebraisch sind, muss also π transzendent sein.* —