Übungsblatt 10: Körpererweiterungen und Automorphismen

1. Grundlagen

1.1. Zeigen Sie, dass die Menge der Zahlen $\{\log(p) : p \text{ Primzahl }\}$ im $\mathbb{Q}$-Vektorraum $\mathbb{R}$ linear unabhängig ist. Folgern Sie $|\mathbb{R} : \mathbb{Q}| = \infty$.

Lösungshinweise: — *Sei $\sum_{i=1}^n \frac{a_i}{b_i}\log(p_i) = 0$ mit $a_i, b_i \in \mathbb{Z}$ ($b_i \neq 0$) und p_i verschiedene Primzahlen. Durch Multiplikation mit dem Hauptnenner, kann man erreichen, dass wir $\sum_{i=1}^n c_i \log(p_i) = 0$ mit $c_i \in \mathbb{Z}$ erreichen. Dann folgt mit den Exponentialgesetzen $0 = \sum_{i=1}^n c_i \log(p_i) = \log(\prod_{i=1}^n p_i^{c_i})$, also $1 = \prod_{i=1}^n p_i^{c_i}$. Dies kann man zu $\prod_{i=1, c_i<0}^n p_i^{-c_i} = \prod_{i=1, c_i\geq 0}^n p_i^{c_i}$ umschreiben. Weil $\mathbb{Z}$ ein faktorieller Ring ist, folgt damit $c_i = 0$ für alle $1 \leq i \leq n$ und somit auch $a_i = 0$, was zu zeigen war.* —

1.2. (a) Zeigen Sie, dass die Menge der algebraischen Zahlen über $\mathbb{Q}$ abzählbar ist.
(b) Zeigen Sie, dass die Menge der reellen Zahlen überabzählbar ist.
(c) Folgern Sie die Existenz von reellen transzendenten Zahlen.

Lösungshinweise: —

(a) *Jedes Polynom ist durch seine Koeffizienten festgelegt und somit kann ein Polynom in $\mathbb{Q}[X]$ vom Grad n durch einen Vektor aus $\mathbb{Q}^{n+1}$ eindeutig beschrieben werden. Damit ist also die Menge aller Polynome über $\mathbb{Q}$ gleichmächtig zu $\bigcup_{n=1}^\infty \mathbb{Q}^n$ und als abzählbare Vereinigung abzählbarer Mengen abzählbar. Jedes Polynom hat aber auch nur endlich viele Nullstellen, so dass also die Menge aller algebraischen Zahlen abzählbar ist.*

(b) *Man lese das Diagonalfolgenargument von Cantor nach (s. Analysis 1).*

(c) *Da es nur abzählbar viele algebraische Zahlen gibt, die Menge aller reeller (und komplexer) Zahlen aber überabzählbar ist, muss es transzendente (= nichtalgebraische) Zahlen geben.*

—

2. Körpererweiterungen

S 2.1. (2 Punkte) Sind die Erweiterungen $\mathbb{Q}[\sqrt{7}]$ und $\mathbb{Q}[\sqrt{11}]$ isomorph?

Lösungshinweise: — *Angenommen es gäbe einen Isomorphismus $\kappa : \mathbb{Q}[\sqrt{7}] \to \mathbb{Q}[\sqrt{11}]$. Dann muss es $a, b \in \mathbb{Q}$ mit $\kappa(\sqrt{7}) = a + b\sqrt{11}$ geben. Es folgt dann $7 = \kappa(7) = \kappa(\sqrt{7}^2) = \kappa(\sqrt{7})^2 = (a + b\sqrt{11})^2$. Umgeformt ergibt sich $2ab\sqrt{11} = 7 - a^2 - 11b^2$. Da $\sqrt{11}$ irrational ist, kann diese Gleichung nur für $a = 0$ oder $b = 0$ erfüllt sein. Im ersten Fall folgt $7 = 11b^2$ und daraus $7m^2 = 11n^2$, wenn $b = \frac{n}{m}$. Diese Gleichung ist in $\mathbb{Z}$ wegen der eindeutigen Primfaktorzerlegung nicht lösbar. Im zweiten Fall entsteht $7 = a^2$, die in $\mathbb{Q}$ ebenfalls unlösbar ist. Damit sind $\mathbb{Q}[\sqrt{7}]$ und $\mathbb{Q}[\sqrt{11}]$ nicht isomorph.* —

2.2. Bestimmen Sie die Dimension von $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ über $\mathbb{Q}$.
Finden Sie fünf Zwischenkörper der Körpererweiterung $\mathbb{Q}[\sqrt{2}, \sqrt{3}]|\mathbb{Q}$.

Lösungshinweise: — *Es ist $1 < |\mathbb{Q}[\sqrt{2}] : \mathbb{Q}| \leq 2$. Die erste Ungleichung folgt daraus, dass $\sqrt{2}$ irrational ist und die zweite aus $\sqrt{2}^2 \in \mathbb{Q}$. Ebenso ist $|\mathbb{Q}[\sqrt{3}] : \mathbb{Q}| = 2$. Der dritte Körper hat Dimension 4, da mit dem Gradsatz $|\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}| = |\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{2}]| \cdot |\mathbb{Q}[\sqrt{2}] : \mathbb{Q}|$ gilt und der erste Faktor auch 2 ist, wie die folgende Rechnung zeigt. Es ist wegen $\sqrt{3}^2 \in \mathbb{Q}$ wieder $|\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{2}]| \leq 2$ aber $\sqrt{3} = a + b\sqrt{2}$ hat keine Lösung mit $a, b \in \mathbb{Q}$, wie man sieht, wenn man beide Seiten quadriert und wie bei Aufgabe 2.1 vorgeht. Somit folgt $|\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{2}]| > 1$.*
Wir haben die fünf Zwischenkörper $\mathbb{Q}, \mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{3}], \mathbb{Q}[\sqrt{6}], \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Diese sind unterschiedlich, wie

man am Grad erkennt (es ist wie oben $|\mathbb{Q}[\sqrt{6}]:\mathbb{Q}|=2$) oder indem man zwei dieser Körper vereinigt und sieht, dass die Vereinigung echt größer wird. —

2.3. Sei $a+bi\in\mathbb{C}$ algebraisch über $\mathbb{Q}$. Zeigen Sie, dass dann auch $a-bi$, a und b algebraisch über $\mathbb{Q}$ sind.

Lösungshinweise: — *Wenn $a+bi$ Nullstelle eines reellen Polynoms ist, dann auch $a-bi$ (siehe Analysis 1 oder Aufgabe 4.3 mit σ = komplexe Konjugation). Daraus folgt aber, dass $a=\frac{1}{2}(a+bi+a-bi)$ und $bi=\frac{1}{2}(a+bi-(a-bi))$ algebraisch sind, weil die Menge der algebraischen Zahlen einen Körper bilden. Wenn aber bi Nullstelle eines Polynoms $P=X^n+a_{n-1}X^{n-1}+\ldots+a_0$ mit rationalen Koeffizienten $a_i\in\mathbb{Q}$ ist, so ist b Nullstelle der Polynome $Re(P(iX))$ und $Im(P(iX))$ und damit algebraisch, da eines der Polynome nichttrivial sein muss.* —

V 2.4. Sei $E|K$ eine Körpererweiterung mit $|E:K|<\infty$.
(a) Es ist E algebraisch über K und $E=K[\alpha_1,\ldots,\alpha_r]$ für geeignete $\alpha_i\in E$.
(b) Sei $|E:K|=p$ eine Primzahl, dann gilt sogar $E=K[\xi]$ für ein $\xi\in E\backslash K$.
(c) Sei $|E:K|=2$ und $\mathrm{char}(K)\neq 2$. Zeigen Sie, dass es ein Element $a\in E$ gibt mit $a\notin K$, $a^2\in K$. Somit ist $E=K[a]$ und $(1,a)$ ist eine Basis von E über K.

Lösungshinweise: —

(a) *Wir führen eine Induktion über den Grad $|E:K|$ der Erweiterung. Wenn $|E:K|=1$, dann ist $E=K$ und $r=0$. Sonst gibt es ein $\alpha_1\in E\backslash K$ und dann gilt nach Gradsatz $|E:K|=|E:K[\alpha_1]|\cdot|K[\alpha_1]:K|$. Wegen $\alpha_1\notin K$ ist der zweite Faktor >1. Damit ist $|E:K[\alpha_1]|<|E:K|$ und nach Induktion existieren $\alpha_2,\ldots,\alpha_r$ mit $E=K[\alpha_1][\alpha_2,\ldots,\alpha_r]=K[\alpha_1,\ldots,\alpha_r]$, was zu zeigen war.*

(b) *Es gilt wie in (a) $p=|E:K|=|E:K[\alpha_1]|\cdot|K[\alpha_1]:K|$. $|K[\alpha_1]:K|$ ist also ein Teiler >1 von p, also $|K[\alpha_1]:K|=p$. Daraus folgt aber $|E:K[\alpha_1]|=1$ und damit $E=K[\alpha_1]$. Wähle $\xi=\alpha_1$.*

(c) *Zuerst finden wir ein ξ wie in Teil (b), so dass $E=K[\xi]$. Dann betrachte $(x+y\xi)^2=x^2+2xy\xi+y^2\xi^2$. Es ist $\xi^2=u+v\xi$ mit geeigneten $u,v\in K$ und damit $(x+y\xi)^2=x^2+uy^2+(2xy+vy^2)\xi$. Wählt man nun x,y so, dass $2xy+vy^2=0$ und $y\neq 0$, so erhalten wir das gesuchte Element a. Man kann zum Beispiel $y=1$ und $x=-v/2$ wählen.*

—

2.5. Eine Erweiterung $E|K$ ist genau dann algebraisch, wenn jeder Teilring R mit $K\subset R$ auch ein Körper ist.

Lösungshinweise: — *Wenn wir eine Erweiterung $E|K$ mit einem $\xi\in E$ haben, das transzendent über K ist, so ist $K[\xi]$ ein Unterring von E, der kein Körper ist, denn das Element ξ hat darin kein Inverses. Ansonsten hätte man $\xi^{-1}=P(\xi)$ für ein Polynom P und damit wäre ξ Nullstelle des Polynoms $PX-1$.*
Ist die Erweiterung andererseits algebraisch, so gibt es zu jedem Element $a\in E$ ein Polynom $Q=X^n+a_{n-1}X^{n-1}+\ldots a_0$ mit $Q(a)=0$. Damit ist dann das Inverse $a^{-1}=\frac{-1}{a_0 a}(Q(a)-a_0)$ durch ein Polynom in a darstellbar. Nimmt man also einen Teilring $K\subset R\subset E$ her, so ist mit jedem Element a von R auch sein Inverses in R enthalten. R ist also ein Körper. —

V 2.6. Sei $E|K$ eine Körpererweiterung und $\alpha,\beta\in E$ seien algebraisch über K.
(a) Zeigen Sie, dass $|K[\alpha,\beta]:K|\leq|K[\alpha]:K|\cdot|K[\beta]:K|$ gilt.
(b) Sind $|K[\alpha]:K|$ und $|K[\beta]:K|$ teilerfremd, so gilt in (a) Gleichheit.

Lösungshinweise: —

(a) *Es ist nach Gradsatz $|K[\alpha,\beta]:K|=|K[\alpha,\beta]:K[\beta]|\cdot|K[\beta]:K|$. Es reicht also zu zeigen, dass $|K[\alpha,\beta]:K[\beta]|\leq|K[\alpha]:K|$ gilt. Es ist $K[\alpha,\beta]=K[\beta][\alpha]$. Jedes Element in diesem Körper lässt sich als Linearkombination von Potenzen von α mit Koeffizienten in $K[\beta]$ darstellen. Die*

Elemente in $K[\alpha]$ sind auch Polynome in α, aber mit Koeffizienten aus K. Eine Basis des ersten K-Vektorraumes ist also auf jeden Fall in zweiten K-Vektoraum linear unabhängig (man hat weniger mögliche Koeffizienten). Also gilt die gewünschte Ungleichung.

(b) *Sowohl $K[\alpha]$, als auch $K[\beta]$ sind Unterkörper von $K[\alpha,\beta]$. Nach dem Gradsatz sind also $|K[\alpha]:K|$ und $|K[\beta]:K|$ Teiler von $|K[\alpha,\beta]:K|$. Da die beiden Zahlen teilerfremd sind folgt, dass das Produkt $|K[\alpha]:K|\cdot|K[\beta]:K|$ ein Teiler von $|K[\alpha,\beta]:K|$ ist. Mit der Ungleichung aus (a) folgt dann sogar Gleichheit.*

—

2.7. Man bestimme die algebraischen Erweiterungen von $\mathbb{C}$ und von $\mathbb{R}$.
Man gebe Beispiele nicht-algebraischer Erweiterungen von $\mathbb{C}$ und von $\mathbb{R}$.

Lösungshinweise: — *Da $\mathbb{C}$ algebraisch abgeschlossen ist, ist jede algebraische Erweiterung von $\mathbb{C}$ einfach wieder $\mathbb{C}$ selbst. Über $\mathbb{R}$ sind die irreduziblen Polynome entweder linear oder quadratisch (siehe Aufgabe 1.1 auf Blatt 4). Damit ist jede algebraische Erweiterung trivial, also $\mathbb{R}$ selbst, oder entsteht durch Adjunktion von Nullstellen von irreduziblen quadratischen Polynomen. Wenn aber $a+bi$ in einer Erweiterung von $\mathbb{R}$ enthalten ist, so auch $i=((a+bi)-a)/b$. Also ist die Erweiterung gerade $\mathbb{C}$.*
Da die Körper der rationalen Funktionen $\mathbb{R}(X)$ und $\mathbb{C}(X)$ echte Erweiterungen von $\mathbb{R}$ bzw. $\mathbb{C}$ sind, müssen diese nach den vorherigen Überlegungen nicht-algebraisch sein. Man sieht es auch daran, dass alle Potenzen des Elementes X linear unabhängig sind. —

2.8. Angenommen $e\in\mathbb{R}$ sei transzendent über $\mathbb{Q}$. Ist e dann auch transzendent über jeder algebraischen Erweiterung von $\mathbb{Q}$?

Lösungshinweise: — *Angenommen, das Element e sei algebraisch über der algebraischen Erweiterung E von $\mathbb{Q}$. Es gibt also ein Polynom P mit Koeffizienten $a_0,\dots,a_n\in E$, so dass $P(e)=0$. Dann ist e aber auch algebraisch über dem Körper $\mathbb{Q}[a_0,\dots,a_n]$ endlichen Grades. Insbesondere folgt mit dem Gradsatz $|\mathbb{Q}[a_0,\dots,a_n,e]:\mathbb{Q}| = |\mathbb{Q}[a_0,\dots,a_n,e]:\mathbb{Q}[a_0,\dots,a_n]|\cdot|\mathbb{Q}[a_0,\dots,a_n]:\mathbb{Q}|<\infty$. Nach Aufgabe 2.4. ist dann $\mathbb{Q}[a_0,\dots,a_n,e]\mid\mathbb{Q}$ algebraisch, also insbesondere auch das Element e.* —

2.9. Jede einfache transzendente Körpererweiterung $E|K$ hat unendlich viele Zwischenkörper.

Lösungshinweise: — *Sei $E=K(\xi)$. Betrachte $K(\xi)>K(\xi^2)>K(\xi^4)>\dots$. Dies sind alles verschiedene Unterkörper von E. Es reicht $K(\xi)>K(\xi^2)$ zu zeigen. Der Rest ist Induktion. Falls $\xi\in K(\xi^2)$ gelten würde, hätten wir $\xi=P(\xi^2,\xi^{-2})$ für ein Polynom $P(X,Y)\in K[X,Y]$. Es ist $X^nP(X,X^{-1})$ ein Polynom, wenn n groß genug gewählt wird. Damit wäre aber ξ Nullstelle des nichttrivialen Polynoms $X^{2n}P(X^2,X^{-2})-X^{2n+1}$. Widerspruch zur Transzendenz!* —

3. Zerfällungskörper

3.1. Sei $\xi=e^{2\pi i/p}$ eine Nullstelle des Polynoms X^p-1 für eine Primzahl p.
Ist $\mathbb{Q}[\xi]$ der Zerfällungskörper von X^p-1 über $\mathbb{Q}$?

Lösungshinweise: — *Alle Nullstellen von X^p-1 sind von der Form ξ^k, also in $\mathbb{Q}[\xi]$ enthalten. Da ξ selbst auch eine Nullstelle ist, ist $\mathbb{Q}[\xi]$ der Zerfällungskörper von X^p-1 über $\mathbb{Q}$.* —

S 3.2. (6 Punkte)

(a) Zeigen Sie, dass $\mathbb{Q}[\sqrt[3]{2},j]$ mit $j=e^{2\pi i/3}$ ein Zerfällungskörper von X^3-2 über $\mathbb{Q}$ ist.

(b) Welche Dimension haben $\mathbb{Q}[\sqrt[3]{2}], \mathbb{Q}[j\sqrt[3]{2}]$ und $\mathbb{Q}[j^2\sqrt[3]{2}]$ als $\mathbb{Q}$-Vektorräume? Bestimmen Sie eine Basis von $\mathbb{Q}[\sqrt[3]{2}]$ über $\mathbb{Q}$.
(c) Warum ist $\mathbb{Q}[\sqrt[3]{2}]$ kein Zerfällungskörper von X^3-2 über $\mathbb{Q}$?
(d) Finden Sie das Minimalpolynom von j über $\mathbb{Q}$.
(e) Bestimmen Sie die Dimension von $\mathbb{Q}[j]$ und $\mathbb{Q}[\sqrt[3]{2}, j]$ über $\mathbb{Q}$.
(f) Bestimmen Sie sechs Zwischenkörper der Erweiterung $\mathbb{Q}[\sqrt[3]{2}, j]|\mathbb{Q}$.

Lösungshinweise: —

(a) *Die Nullstellen von X^3-2 sind $\sqrt[3]{2}, j\sqrt[3]{2}$ und $j^2\sqrt[3]{2}$, also alle in $\mathbb{Q}[\sqrt[3]{2}, j]$ enthalten. Es gilt aber auch, dass $\sqrt[3]{2}$ und $j = \frac{j\sqrt[3]{2}}{\sqrt[3]{2}}$ im Zerfällungskörper enthalten sein müssen. Damit ist alles gezeigt.*
(b) *Das Polynom X^3-2 ist irreduzibel und damit das Minimalpolynom seiner Nullstellen. Nach Satz 12C8 ist der Grad der Erweiterungen $\mathbb{Q}[\sqrt[3]{2}], \mathbb{Q}[j\sqrt[3]{2}]$ und $\mathbb{Q}[j^2\sqrt[3]{2}]$ gerade der Grad des Minimalpolynoms, also 3.*
(c) *Die komplexe Nullstelle $j\sqrt[3]{2}$ liegt nicht in $\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$, also enthält $\mathbb{Q}[\sqrt[3]{2}]$ nicht alle Nullstellen von X^3-2 und ist damit nicht der Zerfällungskörper.*
(d) *Es ist $j^3 = 1$ und somit ist das Minimalpolynom ein Teiler von $X^3-1 = (X-1)(X^2+X+1)$. Der erste Faktor ist es offenbar nicht. Der zweite Faktor ist nach Vorlesung irreduzibel und in $\mathbb{Q}[X]$ enthalten, also das Minimalpolynom von j über $\mathbb{Q}$.*
(e) *Aus dem vorherigen Teil und Satz 12C8 folgt, dass die Dimension $|\mathbb{Q}[j] : \mathbb{Q}| = 2$ ist. Wegen $|\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}| = 3$ und Aufgabe 2.8 folgt $|\mathbb{Q}[\sqrt[3]{2}, j] : \mathbb{Q}| = 6$.*
(f) *Wir haben die trivialen Zwischenkörper $\mathbb{Q}$ und $\mathbb{Q}[\sqrt[3]{2}, j]$. Dann gibt es noch $\mathbb{Q}[j], \mathbb{Q}[\sqrt[3]{2}], \mathbb{Q}[j\sqrt[3]{2}]$ und $\mathbb{Q}[j^2\sqrt[3]{2}]$. Durch die Dimension können wir alle bis auf die letzten drei voneinander unterscheiden. Weiter liegt $\mathbb{Q}[\sqrt[3]{2}]$ vollständig in $\mathbb{R}$, was für $\mathbb{Q}[j\sqrt[3]{2}]$ und $\mathbb{Q}[j^2\sqrt[3]{2}]$ nicht erfüllt ist. Diese beiden sind aber auch nicht gleich, denn die Vereinigungsmenge ergibt $\mathbb{Q}[j\sqrt[3]{2}, j^2\sqrt[3]{2}] = \mathbb{Q}[\sqrt[3]{2}, j]$, da $j = \frac{j^2\sqrt[3]{2}}{j\sqrt[3]{2}}$ und damit auch $\sqrt[3]{2}$ darin enthalten sind.*

—

3.3. Man zeige, dass $E = \mathbb{Q}[i, \sqrt[4]{2}]$ ein Zerfällungskörper von X^4+2 über $\mathbb{Q}$ ist. Ist E auch ein Zerfällungskörper von X^4-2 über $\mathbb{Q}$? Man bestimme den Grad $|E : \mathbb{Q}|$ und finde eine Basis von E über $\mathbb{Q}$.

Lösungshinweise: — *Die Nullstellen von X^4+2 sind $k\sqrt[4]{2}, k^3\sqrt[4]{2}, k^5\sqrt[4]{2}, k^7\sqrt[4]{2}$ mit $k = e^{2\pi i/8} = \frac{1+i}{\sqrt{2}}$.*
Es ist $i = k^2 = \frac{k^3\sqrt[4]{2}}{k\sqrt[4]{2}}$ im Zerfällungskörper enthalten. Da $\sqrt{2} = k^3\sqrt[4]{2} \cdot k^5\sqrt[4]{2}$, folgt auch das $k = \frac{1+i}{\sqrt{2}}$ im Zerfällungskörper liegt. Andererseits sind alle Nullstellen offenbar durch k und $\sqrt[4]{2}$ darstellbar, also liegt der Zerfällungskörper auch in E.
Die Nullstellen von X^4-2 sind $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$ und somit ist der Zerfällungskörper offenbar in E enthalten. Andererseits sind auch $i = \frac{i\sqrt[4]{2}}{\sqrt[4]{2}}$ und $\sqrt[4]{2}$ im Zerfällungskörper enthalten und somit auch ganz E. Die beiden unterschiedlichen Polynome haben also denselben Zerfällungskörper.
Es ist $|E : \mathbb{Q}| = 8$ mit Basis $(1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}, i, i\sqrt[4]{2}, i\sqrt[4]{4}, i\sqrt[4]{8})$. Dazu reicht er zu zeigen, dass die Elemente $1, \sqrt[4]{2}, \sqrt[4]{4}$ und $\sqrt[4]{8}$ über $\mathbb{Q}$ unabhängig sind, da die anderen Elemente rein imaginäre Vielfache der ersten vier Zahlen sind. Nun ist aber X^4-2 irreduzibel (Eisenstein) und somit kann es keine nichttriviale Linearkombination der Potenzen < 4 geben, da dies zu einem echten Faktor des Polynoms führen würde. —

4. KÖRPERAUTOMORPHISMEN

4.1. Seien K und L Körper und $\sigma : K \to L$ ein Körperhomomorphismus. Zeigen Sie, dass σ injektiv ist und K und L die gleiche Charakteristik haben.

Lösungshinweise: — *Es ist* $1=\sigma(1)=\sigma(a\cdot a^{-1})=\sigma(a)\cdot\sigma(a^{-1})$ *für alle* $a\in K^\times$. *Damit ist* $\sigma(a)\neq 0$ *und* σ *injektiv. Wenn* $pa=0$ *in K, dann ist auch* $0=\sigma(pa)=p\sigma(a)$. *Insbesondere ist* $0=p\sigma(1)=p\cdot 1$. *Also hat L dann auch Charakteristik p. Umgekeht folgt aus* $p\cdot 1=0$ *in L und der Injektivität mit einem ähnlichen Argument, dass K dieselbe Charakteristik wie L hat.*
Falls K Charakteristik 0 *hat, bekommen wir wegen der Injektivität, dass das Bild des Primkörpers* $\mathbb{Q}$ *wieder isomorph zu* $\mathbb{Q}$ *ist und damit auch die Charakteristik von L null ist.* —

4.2. Sei K ein Körper und $\sigma: K\to K$ ein Körperautomorphismus.

(a) Zeigen Sie, dass σ den Primkörper von K punktweise festlässt. Folgern Sie daraus, dass $\mathbb{F}_p$ und $\mathbb{Q}$ nur die Identität als Körperautomorphismen haben.

(b) Zeigen Sie weiter, dass auch $\mathrm{Aut}(\mathbb{R})=\{\mathrm{id}_\mathbb{R}\}$ gilt. *Hinweis:* Es ist $x\geq 0\Leftrightarrow \exists\, r\in\mathbb{R}: x=r^2$. Folgern Sie daraus, dass σ stetig ist.

(c) Bestimmen Sie alle Automorphismen $\sigma:\mathbb{C}\to\mathbb{C}$ mit $\sigma(\mathbb{R})=\mathbb{R}$.

Lösungshinweise: —

(a) *Es ist nach Definition* $\sigma(0)=0$ *und* $\sigma(1)=1$. *Daraus folgert man zuerst mit Induktion, dass* $\sigma(n)=n$ *für alle* $n\in\mathbb{N}$. *Aus* $\sigma(n)+\sigma(-n)=\sigma(n-n)=0$ *folgt die Aussage dann für alle* $n\in\mathbb{Z}$. *Aus* $\sigma(n)\cdot\sigma(1/n)=\sigma(n/n)=1$ *folgt, dass* $\sigma(1/n)=1/\sigma(n)$ *und mit Multiplikativität dann* $\sigma(q)=q$ *für alle* $q\in\mathbb{Q}$. *Falls der Körper Charakteristik* $p>0$ *hat muss man ein paar Fallunterscheidungen mehr machen. Die Idee ist aber genau dieselbe.*
Wenn also $K=\mathbb{Q}$ *oder* $K=\mathbb{F}_p$, *so ist* $\sigma=\mathrm{id}$.

(b) *Wenn* $x\geq 0$, *dann ist* $x=r^2$ *für ein* $r\in\mathbb{R}$. *Damit ist dann* $\sigma(x)=\sigma(r^2)=\sigma(r)^2\geq 0$. *Ist* $x\leq y$, *so ist* $0\leq\sigma(y-x)=\sigma(y)-\sigma(x)$. σ *erhält also die Ordnung von* $\mathbb{R}$. *Für alle* $q,r\in\mathbb{Q}$ *mit* $q\leq x\leq r$ *gilt also* $q=\sigma(q)\leq\sigma(x)\leq\sigma(r)=r$. *Da* $\mathbb{Q}$ *dicht in* $\mathbb{R}$ *liegt, folgt* $\sigma(x)=x$.
Alternativ kann aus der obigen Aussage $x\leq y\Rightarrow\sigma(x)\leq\sigma(y)$ *auch gefolgert werden, dass* σ *stetig ist und somit die Identität sein muss, da die Abbildungen auf einer dichten Teilmenge übereinstimmen.*

(c) *Wir wissen, dass die Identität und die komplexe Konjugation solche Körperautomorphismen sind. Kann es noch weitere geben? Zuerst einmal ist* σ *als lineare Abbildung im* $\mathbb{R}$*-Vektorraum* $\mathbb{C}$ *vollständig durch die Bilder der Basis* 1 *und i festgelegt. Weiter haben wir* $\sigma(\mathbb{R})=\mathbb{R}$ *angenommen. Daraus ergibt sich mit Aufgabebenteil (b), dass* $\sigma|_\mathbb{R}=\mathrm{id}_\mathbb{R}$ *gilt. Nun ist aber* $-1=\sigma(-1)=\sigma(i^2)=\sigma(i)^2$, *so dass* $\sigma(i)\in\{i,-i\}$ *folgt. Dies entspricht aber genau den beiden bekannten Automorphismen. Mehr gibt es also nicht.*

—

4.3. Sei $E|K$ eine Körpererweiterung und $\sigma\colon E\to E$ ein Automorphismus von $E|K$. Für alle Polynome $P\in K[X]$ und $x\in E$ gilt $P(\sigma(x))=\sigma(P(x))$. Folgern Sie, dass für eine Nullstelle a von P auch $\sigma(a)$ eine Nullstelle von P ist.

Lösungshinweise: — *Sei* $P(X)=\sum_{i=0}^n a_iX^i$ *mit* $a_i\in K$. *Dann ist* $\sigma(P(x))=\sigma(\sum_{i=0}^n a_ix^i)=\sum_{i=0}^n\sigma(a_i)\sigma(x^i)=\sum_{i=0}^n a_i\sigma(x)^i=P(\sigma(x))$, *wegen* $\sigma|_K=\mathrm{id}$. *Ist also a eine Nullstelle von P, so folgt* $0=\sigma(0)=\sigma(P(a))=P(\sigma(a))$. *Also ist dann auch* $\sigma(a)$ *eine Nullstelle von P.*
Diese Aussage kann bei der Suche nach Körperautomorphismen sehr hilfreich sein! —

V 4.4. (a) Ist $E|K$ algebraisch, dann ist jeder Körperhomomorphismus $\sigma\colon E\to E$ über K ein Automorphismus.

(b) Geben Sie zu einem Körper K eine Erweiterung $E|K$ und einen Körperhomomorphismus $\sigma\colon E\to E$ über K an, der kein Automorphismus ist.

Lösungshinweise: —

(a) *Sei $\sigma : E \to E$ ein Körperhomomorphismus mit $\sigma|_K = \mathrm{id}$. Sei weiter ein $a \in E$ gegeben. Da $E \mid K$ algebraisch ist, existiert ein Polynom $P \in K[X]$ mit $P(a) = 0$. Nach Aufgabe 4.3 bildet σ die Nullstellen des Polynoms auf Nullstellen des Polynoms ab und nach Aufgabe 4.1 ist σ injektiv. Da die Menge der Nullstellen von P endlich ist, folgt dass σ auf der Menge Nullstellen auch surjektiv ist. Insbesondere ist a selbst im Bild von σ. Das war zu zeigen.*

(b) *Sei $E = K[t]$ und t transzendent über K. Dann ist die lineare Fortsetzung von $\sigma : E \to E : \sigma(t^n) = t^{2n}$ ein Körperhomomorphismus, der kein Automorphismus ist, da nicht surjektiv. Das Einzige, das man nachprüfen muss, ist die Multiplikativität. Dies macht aber keine Probleme.*

—

V 4.5. Sei $K \subset \mathbb{C}$ und $K[a]$ eine Erweiterung von Grad 2 mit $a^2 \in K$ (siehe Aufgabe 2.4). Zeigen Sie, dass $\sigma : K[a] \to K[a] : x + ya \mapsto x - ya$ ein nichttrivialer Körperautomorphismus ist und zeigen Sie, dass $\mathrm{Aut}(K[a]|K) = \{\mathrm{id}, \sigma\}$.

Lösungshinweise: — *Wegen $a \notin K, a^2 \in K$ muss das Minimalpolynom von a gerade $X^2 - a^2$ sein. Jeder Körperhomomorphismus bildet die beiden Nullstellen $a, -a$ aufeinander ab (Aufgabe 4.3), so dass wir nur die beiden Möglichkeiten* id *und σ erhalten. Dass σ wirklich ein nichttrivialer Körperautomorphismus ist, muss man direkt nachrechnen.* —

4.6. Bestimmen Sie alle Automorphismen von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Lösungshinweise: — *Jedes Element von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ lässt sich eideutig schreiben als $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ mit $a, b, c, d \in \mathbb{Q}$. Wir wissen, aus Aufgabe 4.3, dass Nullstellen von Polynomen wieder auf Nullstellen dieser Polynome abgebildet werden. Damit können wir also nur die Vorzeichen der Summanden $\sqrt{2}, \sqrt{3}$ und $\sqrt{6}$ verändern. Wegen $\sqrt{6} = \sqrt{2} \cdot \sqrt{3}$ ist dies für den letzten Term bestimmt, sobald wir die Bilder von $\sqrt{2}$ und $\sqrt{3}$ angeben. Wir erhalten dann $\sigma_1 = \mathrm{id}$, $\sigma_2 : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}$, $\sigma_3 : \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}$ und $\sigma_4 = \sigma_2\sigma_3$. Die beiden mittleren Abbildungen sind nach Aufgabe 4.5 Automorphismen, wenn wir z.B. σ_2 für $K = \mathbb{Q}[\sqrt{3}]$ und $E = \mathbb{Q}[\sqrt{3}][\sqrt{2}]$ ansehen.*
Die Automorphismengruppe von $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ ist also isomorph zu $\mathbb{Z}/_2 \times \mathbb{Z}/_2$. —

5. ENDLICHE KÖRPER

S 5.1. (5 Punkte) Sei $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2 + 1)$.

(a) Begründen Sie, warum $\mathbb{F}_9$ ein Körper ist und $\mathbb{F}_3$ als Teilkörper enthält. Zeigen Sie, dass $(1, X)$ eine Basis von $\mathbb{F}_9$ als Vektorraum über $\mathbb{F}_3$ ist.

(b) Ist die additive Gruppe von $\mathbb{F}_9$ zu $\mathbb{Z}/_9$ oder zu $\mathbb{Z}/_3 \times \mathbb{Z}/_3$ isomorph? Gibt es dann sogar einen Ringisomorphismus zu $\mathbb{Z}/_9$ oder zu $\mathbb{Z}/_3 \times \mathbb{Z}/_3$?

(c) Bestimmen Sie die Ordnungen der Elemente in $\mathbb{F}_9^\times$.

(d) Bestimmen Sie das Bild eines allgemeinen Elementes $a + bX \in \mathbb{F}_9$ unter dem Frobenius-Homomorphismus $x \mapsto x^3$.

(e) Ist $\mathbb{F}_9$ isomorph zu $\mathbb{F}_3[Y]/(Y^2 + Y + 1)$ oder zu $\mathbb{F}_3[Z]/(Z^2 + Z - 1)$? Geben Sie gegebenenfalls einen Isomorphismus κ an. *Hinweis:* Betrachten Sie κ zuerst als lineare Abbildung von $\mathbb{F}_3$-Vektorräumen und zeigen Sie anschließend noch $\kappa(X^2) = \kappa(X)^2$.

Lösungshinweise: —

(a) *Das Polynom $X^2 + 1$ ist irreduzibel (keine Nullstellen in $\mathbb{F}_3$ und Grad ≤ 3) und damit ist der Quotientenring $\mathbb{F}_3[X]/(X^2 + 1)$ nach Korollar 5G9 ein Körper. Die linearen Polynome in $\mathbb{F}_3[X]$ werden dabei injektiv auf 9 verschiedene Restklassen abgebildet. Jedes Element in $\mathbb{F}_9$ hat also einen eindeutigen Repräsentanten der Form $a + bX$ mit $a, b \in \mathbb{F}_3$. Anders gesagt ist $(1, X)$ eine Basis von $\mathbb{F}_9$ über $\mathbb{F}_3$.*

(b) *Als Vektorraum über* $\mathbb{F}_3 = \mathbb{Z}/_3$ *ist die additive Gruppe isomorph zu* $\mathbb{Z}/_3 \times \mathbb{Z}/_3$. *Aber ein Ringisomorphismus kann nicht bestehen, da* $\mathbb{Z}/_3 \times \mathbb{Z}/_3$ *Nullteiler enthält,* $\mathbb{F}_9$ *als Körper aber nicht. Zu* $\mathbb{Z}/_9$ *besteht schon als abelsche Gruppe kein Isomorphismus, also auch nicht als Ring.*

(c) *Man rechnet nach, dass* $(1+X)^4 = -1 \neq 1$ *in* $\mathbb{F}_9$. *Damit hat* $1+X$ *Ordnung* 8 *und erzeugt damit ganz* $\mathbb{F}_9^\times$. *Die Elemente* $1, -1$ *und* $X, -X$ *haben Ordnungen* 1, 2 *und* 4, *wie man durch direkte Rechnung prüft oder indem man sich die Potenzen von* $1+X$ *ansieht. Damit ist* $(\mathbb{F}_9^\times, \cdot) \cong (\mathbb{Z}/_8, +)$.

(d) *Es ist* $(a+bX)^3 = a^3 + 3a^2bX + 3ab^2X^2 + b^3X^3 = a^3 + b^3X^3 = a - bX$ *wegen* $X^2 = -1$ *und* $a^3 = a$ *für alle* $a \in F_3$ *nach dem kleinen Satz von Fermat.*

(e) *Es gilt* $Y^2 + Y + 1 = (Y-1)^2$ *über* $\mathbb{F}_3$ *und somit hat* $\mathbb{F}_3[Y]/(Y^2+Y+1)$ *den Nullteiler* $Y-1$ *und kann nicht zu* $\mathbb{F}_9$ *isomorph sein.*
Das Polynom $Z^2 + Z - 1$ *ist wie* $X^2 + 1$ *irreduzibel und somit ist* $\mathbb{F}_3[Z]/(Z^2+Z-1)$ *auch ein Körper mit* 9 *Elementen. Ein Isomorphismus* κ *ist schon durch die Wahl* $\kappa(X) = Z + 2$ *festgelegt, wenn wir ihn linear auf den* $\mathbb{F}_3$*-Vektorraum* $\mathbb{F}_9$ *fortsetzen. Dieser ist wohldefiniert, da das Polynom* $X^2 + 1$ *dadurch auf* $Z^2 + Z - 1$ *abgebildet wird. Die Invertierbarkeit folgt durch Angabe der inversen Abbildung* $Z \mapsto X - 2$. *Es bleibt nur noch die Multiplikativität zu prüfen. Es ist aber* $\kappa(aX) = a\kappa(X)$ *für alle* $a \in \mathbb{F}_3$ *nach Linearität und somit ist nur noch* $\kappa(X^2) = \kappa(X)^2$ *nachzuweisen. Dies rechnet man aber direkt nach:* $\kappa(X^2) = \kappa(-1) = -1$ *und* $\kappa(X)^2 = (Z+2)^2 = Z^2 + 4Z + 4 = -1$.

—

5.2. Zeigen Sie, dass ein endlicher Körper nie algebraisch abgeschlossen sein kann.

Hinweis: Jeder endliche Körper F hat eine Primzahl p als Charakteristik. Zu dem Polynom $P = X^{p^n} - X$ in $F[X]$ berechne man $\operatorname{ggT}(P, P')$ und leite hieraus die Anzahl der verschiedenen Nullstellen von P ab.

Lösungshinweise: — *Es ist* $P' = pX^{p^n-1} - 1 = -1$ *und somit* $\operatorname{ggT}(P, P') = 1$. *Das bedeutet, dass jede Nullstelle von P einfach ist. Wählt man nun n so groß, dass* p^n *größer ist als die Anzahl der Elemente des Körpers, so muss das Polynom auch nichtlineare irreduzible Faktoren enthalten, da jedes lineare Polynom nach Vorüberlegung nur einmal als Faktor auftreten kann. Damit ist der Körper aber nicht algebraisch abgeschlossen.* —

5.3. Geben Sie einen unendlichen Körper K mit Charakteristik $p > 0$ an, so dass der Frobenius-Homomorphismus $x \mapsto x^p$

(a) injektiv, aber nicht surjektiv ist,

(b) ein Automorphismus von K ist.

Lösungshinweise: —

(a) *Man betrachte den Körper* $\mathbb{F}_p(X)$ *der rationalen Funktionen über* $\mathbb{F}_p$. *Dieser hat Charakteristik p und besitzt unendlich viele Elemente, wie man direkt nachrechnet. Der Frobenius-Homomorphismus ist nicht surjektiv, weil z.B. das Element X nicht im Bild liegt. Denn wäre* $\left(\frac{R}{Q}\right)^p = X$ *für Polynome* $R, Q \in \mathbb{F}_p[X]$, *so würde* $R^p = XQ^p$ *folgen. Die linke Seite hat aber einen Grad der Form kp und die rechte Seite* $1 + lp$ *mit* $k, l \in \mathbb{N}$. *Dies ist dann der gewünschte Widerspruch.*

(b) *Nimmt man nun aber den algebraischen Abschluss L von* $\mathbb{F}_p(X)$, *so wird der Frobenius-Homomorphismus surjektiv. Denn zu jedem* $a \in L$ *gibt es dann ein* $b \in L$ *mit* $b^p = a$, *weil das Polynom* $X^p - a$ *eine Nullstelle in L besitzt. (Warum ist das b sogar eindeutig?)*

—