Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 08/09 9. Dezember 2008

Algebra

9. Übung mit Lösungshinweisen

Aufgabe 41 Es seien R, S Integritätsbereiche, $\mathbb{K}, \mathbb{L}$ Körper und $f : \mathbb{K} \to \mathbb{L}$ ein Körperhomomorphismus.

(a) Zeige, daß $\mathbb{K}$ und $\mathbb{L}$ dieselbe Charakteristik besitzen.

(b) Kann es einen Ringhomomorphismus $g : R \to S$ mit $g(1) = 1$ geben, wenn R und S unterschiedliche Charakteristik haben? Charakterisiere gegebenenfalls die möglichen Charakteristiken von R und S.

Lösung: (a) Hat $\mathbb{L}$ Charakteristik p, so folgt aus $0 = p \cdot 1 = p \cdot f(1) = f(p) = f(0)$, daß p die Charakteristik von $\mathbb{K}$ teilen muß. Hat umgekehrt $\mathbb{K}$ Charakteristik p, so folgt aus obiger Gleichungskette, daß p die Charakteristik von $\mathbb{L}$ teilen muß. Daraus folgt die Behauptung.

(b) Hat R Charakteristik 0, so kann S jede beliebige Charakteristik haben, da es einen unitalen Ringhomomorphismus von $\mathbb{Z}$ nach $\mathbb{Z}_p$ gibt. Hat R Charakteristik p, so muß auch S Charakteristik p haben.

Aufgabe 42 Es sei $\mathbb{L}/\mathbb{K}$ eine Körpererweiterung und Z_1, Z_2 zwei Zwischenkörper. Das *Kompositum* von Z_1 und Z_2 ist definiert als der kleinste Zwischenkörper der Erweiterung, welcher Z_1 und Z_2 enthält und wird mit $Z_1 \cdot Z_2$ bezeichnet.

(a) Mache Dir klar, daß gilt
$$Z_1 \cdot Z_2 = Z_1(Z_2) = Z_2(Z_1).$$

(b) Zeige, daß, wenn die Erweiterungen $Z_1/\mathbb{K}$ und $Z_2/\mathbb{K}$ algebraisch sind, auch $Z_1 \cdot Z_2/\mathbb{K}$ algebraisch ist.

(c) Zeige, daß aus $[Z_1 : \mathbb{K}] = m$ und $[\mathbb{Z}_2 : \mathbb{K}] = n$ folgt, daß $[Z_1 \cdot \mathbb{Z}_2 : \mathbb{K}] \leq m \cdot n$ gilt. Gilt Gleichheit, wenn m und n teilerfremd sind?

(d) Es seien $u, v \in \mathbb{L}$ algebraisch über $\mathbb{K}$ mit Grad m bzw. n. Zeige, daß dann gilt
$$[\mathbb{K}(u, v) : \mathbb{K}] \leq m \cdot n.$$
Gilt Gleichheit, wenn m und n teilerfremd sind?

Lösung: (a) Es gilt
$$Z_1 \cdot Z_2 = \bigcup \{\mathbb{K} \subseteq Z \subseteq \mathbb{L} : Z \text{ Körper und } Z_1 \cup Z_2 \in Z\}.$$
Da $Z_1(Z_2)$ der kleinste Oberkörper von Z_1 ist, welcher alle Elemente aus Z_2 enthält, folgt mit symmetrischer Argumentation
$$Z_1(Z_2) = Z_1 \cdot Z_2 = Z_2(Z_1).$$

(b) Sind Z_1 und Z_2 algebraisch über $\mathbb{K}$ und ist $a \in \mathbb{Z}_1$ und $-b \in Z_2$, so ist $a+b, \frac{a}{b} \in \mathbb{K}(a,b)$ (für $b \neq 0$). Nach Skript ist jedes Element aus $\mathbb{K}(a,b)$ algebraisch über $\mathbb{K}$, also sind alle Elemente von $Z_1(Z_2) = Z_1 \cdot Z_2$ algebraisch über $\mathbb{K}$.

(c) Es sei $[Z_1 : \mathbb{K}] = m < \infty$ und $[Z_2 : \mathbb{K}] = n < \infty$. Dann besitzt Z_1 eine $\mathbb{K}$-Basis $B = \{1, b_1, ..., b_{m-1}\}$ und Z_2 eine $\mathbb{K}$-Basis $C = \{1, c_1, ..., c_{n-1}\}$. Ist nun $x \in Z_1 \cdot Z_2 = Z_1(Z_2)$, so besitzt x eine Darstellung als

$$x = f(z_1, ..., z_r),$$

wobei f ein Polynom in r-Unbestimmten mit Koeffizienten aus Z_1 ist und $z_1, ..., z_r \in Z_2$ geeignete Elemente sind. Stellen wir nun die Koeffizienten des Polynoms als Linearkombination der Elemente aus B und die Elemente $z_1, ..., z_r$ als Linearkombination der Elemente aus C dar, so folgt, daß jedes Element von $Z_1(Z_2)$ in der $\mathbb{K}$-linearen Hülle der Elemente von $B \cdot C$ ist. Somit folgt

$$\dim_{\mathbb{K}}(Z_1 \cdot Z_2) \leq m \cdot n.$$

Aus dem Gradsatz folgt weiter, daß

$$[Z_1 \cdot Z_2 : \mathbb{K}] = [Z_1 \cdot Z_2 : Z_1] \cdot [Z_1 : \mathbb{K}] = [Z_1 \cdot Z_2 : Z_1] \cdot m,$$

$$[Z_1 \cdot Z_2 : \mathbb{K}] = [Z_1 \cdot Z_2 : Z_1] \cdot [Z_2 : \mathbb{K}] = [Z_2 \cdot Z_2 : Z_1] \cdot n.$$

Somit teilt der größte gemeinsame Teiler von m und n den Gesamtgrad, sind beide Zahlen teilerfremd, so erhalten wir die Behauptung.

(d) Alle Aussagen folgen aus (c), da $\mathbb{K}(u,v) = \mathbb{K}(u) \cdot \mathbb{K}(v)$ gilt.

Aufgabe 43 Bestimme in folgenden Körpererweiterungen $\mathbb{L}/\mathbb{K}$ für die angegebenen Elemente $a \in \mathbb{L}$ das Minimalpolynom.

(a) $\mathbb{L} = \mathbb{C}$, $\mathbb{K} = \mathbb{Q}$ und $a = i$.

(b) $\mathbb{L} = \mathbb{C}$, $\mathbb{K} = \mathbb{R}$ und $a = i$.

(c) $\mathbb{L} = \mathbb{C}$, $\mathbb{K} = \mathbb{R}$ und $a = \sqrt{7}$.

(d) $\mathbb{L} = \mathbb{C}$, $\mathbb{K} = \mathbb{Q}$ und $a = \sqrt{7}$.

(e) $\mathbb{L} = \mathbb{C}$, $\mathbb{K} = \mathbb{Q}$ und $a = \frac{-1+\sqrt{3}\cdot i}{2}$.

LÖSUNG: (a) $m_{i,\mathbb{Q}} = X^2 + 1$.

(b) $m_{i,\mathbb{R}} = X^2 + 1$.

(c) $m_{\sqrt{7},\mathbb{R}} = X - \sqrt{7}$.

(d) $m_{\sqrt{7},\mathbb{Q}} = X^2 - 7$.

(e) $m_{\frac{i\sqrt{3}-1}{2},\mathbb{Q}} = X^2 + X + 1$.
Das angegebene Polynom ist irreduzibel und hat a als Nullstelle. Dieses Polynom konstruieren wir wie folgt:

$$\left(a + \frac{1}{2}\right)^2 = \left(\frac{i\sqrt{3}}{2}\right)^2 = -\frac{3}{4}.$$

Ausmultiplizieren der linken Seite via binomischer Formel liefert somit

$$a^2 + a + \frac{1}{4} = -\frac{3}{4},$$

somit ist a Nullstelle des angegebenen Polynoms. Die Irreduzibilität folgt leicht daher, daß das angegebene Polynom keine reelle Nullstelle, also auch keine rationale, haben kann.

Aufgabe 44 Bestimme den Erweiterungsgrad folgender Erweiterungen

(a) $\mathbb{Q}(\sqrt[17]{42})/\mathbb{Q}$,

(b) $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$,

(c) $\mathbb{Q}(i,\sqrt{3},\eta)/\mathbb{Q}$, wobei η eine echte komplexe dritte Einheitswurzel sei.

LÖSUNG: (a) $X^{17}-42$ ist nach Eisenstein irreduzibel, also ist das Polynom das Minimalpolynom und wir erhalten Grad 17.

(b) Da X^2-2 irreduzibel in $\mathbb{Q}[X]$ ist, folgt mit dem Gradsatz

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot 2.$$

Somit teilt 2 den Grad der Erweiterung.
Wir behaupten, daß X^2-3 irreduzibel in $\mathbb{Q}(\sqrt{2})[X]$ ist. Angenommen, X^2-3 hätte in diesem Körper eine Nullstelle. Dann existieren rationale Zahlen a,b mit

$$(a+\sqrt{2}b)^2-3=0.$$

Ausrechnen liefert die Gleichung

$$a^2+2\sqrt{2}a\cdot b+2b^2-3=0.$$

Somit folgt $a=0$ oder $b=0$. Erster Fall $a=0$, dann gilt

$$2b^2=3,$$

das geht nicht, da alle Primteiler von b^2 einen geraden Exponenten haben müssen.
Zweiter Fall $b=0$, dann gilt $a^2=3$, eine Gleichung, die in $\mathbb{Q}$ keine Lösung hat. Somit existiert die Nullstelle nicht, also ist X^2-3 auch über dem größeren Körper $\mathbb{Q}(\sqrt{2})$ irreduzibel. Damit gilt $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$ und wir erhalten mit dem Gradsatz den Gesamtgrad 4 der Erweiterung.

(c) Wir bemerken $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2$. Da dieser Erweiterungskörper eine Teilmenge der reellen Zahlen ist, ist X^2+1 darüber irreduzibel und wir erhalten

$$[\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}]=4.$$

Da weiter gilt

$$\eta=-\frac{1}{2}+\frac{1}{2}\sqrt{3}\cdot i,$$

gilt $\mathbb{Q}(i,\sqrt{3},\eta)=\mathbb{Q}(i,\sqrt{3})$, also hat diese Körpererweiterung Grad 4.

Aufgabe 45 Sei $a=\sqrt[2]{3}$ und $b=\sqrt[3]{2}$. Bestimme $n:=[\mathbb{Q}(a,b):\mathbb{Q}]$ und ein Polynom in $\mathbb{Q}[X]$ vom Grad $\leq n$, welches $a+b$ als Nullstelle hat.

LÖSUNG: Klar ist, die Polynome

$$f(X)=X^2-3 \quad \text{und} \quad g(X)=X^3-2$$

sind nach Eisenstein irreduzibel in $\mathbb{Q}[X]$. Somit gilt

$$[\mathbb{Q}(a,b):\mathbb{Q}] = [\mathbb{Q}(a,b):\mathbb{Q}(a)]\cdot[\mathbb{Q}(a):\mathbb{Q}] = [\mathbb{Q}(a,b):\mathbb{Q}(a)]\cdot 2,$$

$$[\mathbb{Q}(a,b):\mathbb{Q}] = [\mathbb{Q}(a,b):\mathbb{Q}(b)]\cdot[\mathbb{Q}(b):\mathbb{Q}] = [\mathbb{Q}(a,b):\mathbb{Q}(b)]\cdot 3.$$

Somit hat die Erweiterung mindestens Grad 6. Der Grad ist jedoch auch kleiner gleich 6, da X^3-2 das Minimalpolynom von b über $\mathbb{Q}(a)$ als Teiler besitzt. Somit hat diese Erweiterung Grad 6.
Wir setzen $x := \sqrt[2]{3} + \sqrt[3]{2}$. Damit gilt

$$2 = (x - \sqrt[2]{3})^3 = x^3 - 3\sqrt[2]{3} \cdot x^2 + 9 \cdot x - 3\sqrt[2]{3}.$$

Somit gilt

$$(x^3 + 9 \cdot x - 2) = (3 \cdot x^2 - 3) \cdot \sqrt[2]{3},$$

woraus folgt

$$(x^3 + 9 \cdot x - 2)^2 = 3 \cdot (3 \cdot x^2 - 3)^2.$$

Damit ist

$$f(X) := 3 \cdot (3 \cdot X^2 - 3)^2 - (X^3 + 9 \cdot X - 2)^2$$

ein Polynom geforderten Grades, welches x als Nullstelle hat.

Aufgabe 46 Eine komplexe Zahl $z \in \mathbb{C}$ heißt *algebraische Zahl*, falls z algebraisch über $\mathbb{Q}$ ist und *algebraische ganze Zahl* oder *ganzalgebraische Zahl*, wenn z Nullstelle eines normierten Polynoms aus $\mathbb{Z}[X]$ ist. Zeige:

(a) Falls x eine algebraische Zahl ist, dann existiert ein $n \in \mathbb{Z}$, so daß $n \cdot x$ eine algebraische ganze Zahl ist.

(b) Ist $r \in \mathbb{Q}$ eine algebraische ganze Zahl, so folgt $r \in \mathbb{Z}$.

(c) Ist u eine algebraische ganze Zahl und $n \in \mathbb{Z}$, dann sind $u + n$ und $u \cdot n$ algebraische ganze Zahlen.

Nun wollen wir noch zeigen, daß die Menge aller algebraischen ganzen Zahlen einen Ring bildet.

(d) Sei $M \subseteq \mathbb{C}$ eine abelsche Gruppe, welche von $\{b_1, ..., b_n\} \subseteq \mathbb{C}$ erzeugt werde, es gebe also für jedes $x \in M$ eine Darstellung $x = \sum_{i=1}^{n} \lambda_i \cdot b_i$ mit $\lambda_1, ..., \lambda_n \in \mathbb{Z}$. Zeige, daß eine komplexe Zahl $z \in \mathbb{C}$ eine algebraische ganze Zahl ist, wenn für jedes Element $x \in M$ auch $z \cdot x$ ein Element aus M ist.

(e) Zeige, daß die Menge aller algebraischen ganzen Zahlen einen Ring bildet.

LÖSUNG: (a) OBdA, $f \in \mathbb{Z}[X]$. Ist $f(x) = 0$, so betrachte $g(X) := \frac{X}{n}$, wobei n der Leitkoeffizient von f sei. Dann ist

$$n^{\deg(f)-1} \cdot f(g(X))$$

ein normiertes Polynom, welches $n \cdot x$ als Nullstelle hat.

(b) Ist $r \in \mathbb{Q}$ Nullstelle von

$$f(X) = X^n + ... + a_1 \cdot X + a_0,$$

so wissen wir, daß $r = \frac{p}{q}$ ist, wobei q den Leitkoeffizienten teilt und p den Koeffizienten a_0 teilt. Da der Leitkoeffizient die 1 ist, ist $q = \pm 1$, also ist $r \in \mathbb{Z}$.

(c) Ist $f(u) = 0$ und $n \in \mathbb{Z}$, so hat

$$g(X) := f(X - n)$$

eine Nullstelle $u + n$ und führenden Koeffizienten 1.
Weiter hat

$$h(X) := n^{\deg(f)} \cdot f\left(\frac{X}{n}\right)$$

die Nullstelle $n \cdot u$ und führenden Koeffizienten 1.

(d) Ist die Bedingung für alle $x \in M$ erfüllt, so auch insbesondere für die Erzeuger. Wir erhalten somit für jedes $1 \leq i \leq n$ eine Gleichung

$$z \cdot b_i = \sum_{j=1}^{n} a_{i,j} b_j.$$

Dies können wir umformen zu

$$0 = \sum_{j=1}^{n} (a_{i,j} - \delta_{i,j} \cdot z) b_j.$$

Somit hat das Polynom

$$\det((a_{i,j} - \delta_{i,j} \cdot X)_{i,j})$$

die Zahl z als Nullstelle und ist normiert, da die angegebene Matrix nicht invertierbar in $M_n(\mathbb{Q})$ sein kann.

(e) Sind a und b algebraische ganze Zahlen, so erfüllt a eine normierte polynomiale Gleichung vom Grad m und b eine vom Grad n. Betrachte die Gruppe

$$M := \mathbb{Z}\{a^i \cdot b^j : 0 \leq i \leq m, 0 \leq j \leq n\}.$$

Ist $g \in M$ ein beliebiges Element, so macht man sich leicht klar, daß auch $(a + b) \cdot g$ oder $(a \cdot b) \cdot g$ wieder ein Element von M ist, indem man die polynomialen Gleichungen verwendet, um geeignete Exponenten der Erzeuger zu finden. Damit folgt, daß die algebraischen ganzen Zahlen einen Ring bilden.

Hausübungen

Aufgabe H17 (Algebraische Elemente) Es sei $\mathbb{K}$ ein Körper und $\mathbb{L}/\mathbb{K}$ eine Körpererweiterung.

(a) Zeige, daß der algebraische Abschluß von $\mathbb{K}$ abzählbar ist, wenn $\mathbb{K}$ abzählbar ist.

(b) Zeige, daß die über $\mathbb{K}$ algebraischen Elemente von $\mathbb{L}$ einen Zwischenkörper der Erweiterung $\mathbb{L}/\mathbb{K}$ bilden.

Hinweis: *Die abzählbare Vereinigung abzählbarer Mengen ist wieder eine abzählbare Menge.*

Lösung: (a) Ist $\mathbb{K}$ abzählbar, so auch $\mathbb{K}[X]$ und $\mathbb{K}[(X_i)_{i \in I}]$, wobei I die Menge aller Polynome vom Grad ≥ 1 bezeichne. Dies folgt aus dem Hinweis und der bijektiven Entsprechung

$$K[X] = \bigcup_{n \in \mathbb{N}} \left\{ \{f \in \mathbb{K}[X] : \deg(f) = n\} \cong \mathbb{K}^\times \times \prod_{l=0}^{n-1} \mathbb{K} \right\}$$

und daraus, daß endliche Produkte abzählbarer Mengen wieder abzählbar sind. Analog zeigt man, daß $\mathbb{K}[(X_i)_{i \in I}]$ abzählbar ist.
Somit ist der Quotient L_1 ebenfalls abzählbar, also sind alle Elemente des Erweiterungsturms

$$\mathbb{K} \subseteq L_1 \subseteq L_2 \subseteq ...$$

abzählbare Körper. Somit ist aber auch wieder mit Hinweis der Körper

$$\bigcup_{n \in \mathbb{N}} L_n$$

abzählbar, dies ist aber der algebraische Abschluß.

(b) Sind $u, v \in \mathbb{L}$ algebraisch über $\mathbb{K}$, so sind alle Elemente in $\mathbb{K}(u, v)$ algebraisch über $\mathbb{K}$, insbesondere sind alle erlaubten Summen, Differenzen, Produkte und Quotienten von u, v in $\mathbb{K}(u, v)$, also ebenfalls algebraisch. Damit bilden die algebraischen Elemente aus $\mathbb{L}$ einen Zwischenkörper.

Aufgabe H18 (Kummer-Erweiterung) Es seien $p_1, ..., p_n \in \mathbb{N}$ paarweise verschiedene Primzahlen. Zeige durch Induktion, daß der Bruch $\frac{x}{y}$ für jede teilerfremde Wahl $x, y \in \mathbb{N}$, so daß x kein Quadrat einer ganzen Zahl ist und keine der Primzahlen $p_1, ..., p_n$ eine der Zahlen x oder y in $\mathbb{N}$ teilt, keine Wurzel in $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n})$ besitzt. Folgere dabei für den Erweiterungsgrad

$$[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n}) : \mathbb{Q}] = 2^n$$

und gib eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n})$ an.
Welchen Grad hat also der kleinste Erweiterungskörper von $\mathbb{Q}$, welcher alle Quadratwurzeln natürlicher Zahlen enthält?
Hinweis: *Es kann im Induktionsschritt hilfreich sein, eine $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_{n-1}})$-Basis von $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n})$ zu ermitteln.*

LÖSUNG: **Induktionsanfang:** Betrachte für Primzahlen $p_1 \neq p_2 \in \mathbb{N}$ den Körper $\mathbb{K}_1 := \mathbb{Q}(\sqrt{p_1})$. Sei nun x, y wie in der Aufgabenstellung gewählt. Wir wissen, $\mathbb{K}_1$ besitzt eine $\mathbb{Q}$-Basis $\{1, \sqrt{p_1}\}$, da das Polynom $X^2 - p_1$ in $\mathbb{Q}[X]$ irreduzibel ist. Wäre $\frac{x}{y}$ ein Quadrat in $\mathbb{K}_1$, so erhielten wir

$$\frac{x}{y} = (a + b\sqrt{p_1})^2 = a^2 + 2ab \cdot \sqrt{p_1} + p_1 \cdot b^2.$$

Da $a, b \in \mathbb{Q}$ sind, muß aus der Basiseigenschaft $a \cdot b = 0$ gelten, also $a = 0$ oder $b = 0$.
Ist $a = 0$, so folgt

$$\frac{x}{y \cdot p_1} = b^2,$$

was nicht möglich ist, da weder x noch y durch p_1 teilbar waren. In der eindeutigen Primzahldarstellung der linken Seite muß jeder Primfaktor jedoch mit einem Exponenten aus $2 \cdot \mathbb{Z}$ vorkommen, der Exponent zu p_1 ist aber offensichtlich -1.
Ist $b = 0$, so ist

$$\frac{x}{y} = a^2,$$

was nicht möglich sein kann, da x kein Quadrat war.
Insbesodere ist $p_2 = \frac{p_2}{1}$ eine rationale Zahl, die kein Quadrat in $\mathbb{K}_1$ ist, also ist $X^2 - p_2$ in $\mathbb{K}_1[X]$ ein irreduzibles Polynom. Der Körper $\mathbb{K}_2 := \mathbb{Q}(p_1, p_2)$ ist somit eine Erweiterung von $\mathbb{Q}$ vom Grad 4.
Induktionschritt: Es sei für n der Körper $\mathbb{K}_n := \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$ eine Erweiterung von $\mathbb{Q}$ vom Grad 2^n, und es gelte die Bedingung aus der Aufgabenstellung. Ist nun

$$\frac{x}{y} = (a + b \cdot \sqrt{p_n})^2 = a^2 + 2ab \cdot \sqrt{p_n} + p_n \cdot b^2,$$

so ist entweder $a = 0$ oder $b = 0$, da $\{1, \sqrt{p_n}\}$ eine $\mathbb{K}_{n-1}$-Basis von $\mathbb{K}_n$ ist.
Ist $a = 0$, so folgt

$$\frac{x}{p_n \cdot y} = b^2.$$

Diese Gleichung hat aber nach Induktionsvorraussetzung keine Lösung $b \in \mathbb{K}_{n-1}$, da der Bruch alle Eigenschaften mit $\mathbb{K}_{n-1}$-Formulierung erfüllt, welche in der Aufgabenstellung gefordert waren.
Ist $b = 0$, so folgt

$$\frac{x}{y} = a^2,$$

eine Gleichung die erst Recht in $\mathbb{K}_{n-1}$ keine Lösung haben kann nach Induktionsvorraussetzung.
Insbesodere ist $p_{n+1} = \frac{p_{n+1}}{1}$ kein Quadrat in $\mathbb{K}_n$, also ist $\sqrt{p_{n+1}} \notin \mathbb{K}_n$, das Polynom $X^2 - p_{n+1}$ in

$\mathbb{K}_n[X]$ irreduzibel und alle Aussagen gezeigt.
Wir erhalten somit für den totalen Erweiterungsgrad

$$[\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n}) : \mathbb{Q}] = 2^n.$$

Weiter bilden die Elemente

$$\left\{ \prod_{k=1}^{n} \sqrt{p_k}^{e_k} \right\}$$

für $e_k \in \{0, 1\}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$.
Ein Erweiterungskörper von $\mathbb{Q}$, welcher alle Quadratwurzeln natürlicher Zahlen enthält, besitzt somit einen höheren Grad als 2^n für jedes $n \in \mathbb{N}$, also ist ein solcher eine unendliche Erweiterung von $\mathbb{Q}$.