23. Normale, separable und galoissche Körpererweiterungen

<u>Satz 214</u> Es sei L/K eine algebraische Körpererweiterung. Dann sind äquivalent:

(i) Jedes irreduzible Polynom $p \in K[X]$, das in L eine Nullstelle besitzt, zerfällt über L in Linearfaktoren

(ii) Ist $\overline{K}$ ein algebraischer Abschluss von K mit der Eigenschaft $L \subseteq \overline{K}$ und $\varphi : L \to \overline{K}$ ein Homomorphismus mit der Eigenschaft $\varphi(x) = x \ \forall x \in K$, so ist $\varphi(L) = L$.

<u>Beweis:</u> (i) $\Rightarrow$ (ii) Ist $a \in L$, so ist a algebraisch über K. Nach Voraussetzung zerfällt das Minimalpolynom $m_{a,K} \in K[X]$ über L in Linearfaktoren, d.h.

$$m_{a,K}(X) = \prod_{i=1}^{n} (X - a_i)$$

für gewisse $a_1 = a, a_2, \dots, a_n \in L$. Aus $\varphi(x) = x \ \forall x \in K$ folgt

$$m_{a,K}(X) = (\overline{\varphi}(m_{a,K}))(X) = \prod_{i=1}^{n} (X - \varphi(a_i))$$

(mit $\overline{\varphi} : L[X] \to \overline{K}[X]$ wie in Lemma 204). Da $\overline{K}[X]$ ein faktorieller Ring ist, müssen $\varphi(a_1) = \varphi(a), \varphi(a_2), \dots, \varphi(a_n)$ eine Permutation von $a_1 = a, a_2, \dots, a_n$ sein. Daher $\exists i, j \in \{1, \dots, n\} : \varphi(a) = \varphi(a_1) = a_i$ und $\varphi(a_j) = a_1 = a$, d.h. $\varphi(a) \in L$ und $a \in \varphi(L)$. Da $a \in L$ beliebig war, folgen $\varphi(L) \subseteq L$ und $L \subseteq \varphi(L)$.

(ii) $\Rightarrow$ (i) Es sei $p \in K[X]$ irreduzibel und $a \in L$ eine Nullstelle von p. Ist $b \in \overline{K}$ irgendeine Nullstelle von p, so gibt es nach Korollar 206 einen Isomorphismus $\varphi : K(a) \to K(b)$ mit den Eigenschaften $\varphi(x) = x \ \forall x \in K$ und $\varphi(a) = b$. Verknüpft man φ mit einer Einbettung $K(b) \hookrightarrow \overline{K}$ (d.h. $K(a) \xrightarrow{\varphi} K(b) \hookrightarrow \overline{K}$) und setzt φ auf L fort (was nach Satz 211 möglich ist), so folgt aus der Voraussetzung $\varphi(L) = L$ und daher $b = \varphi(a) \in L$. Da b eine beliebige Nullstelle von p war, liegen somit alle Nullstellen von p in L. Daher zerfällt p über L in Linearfaktoren.

<u>Definition:</u> Eine algebraische Körpererweiterung L/K, die eine (und damit beide) der Bedingungen aus Satz 214 erfüllt, wird normal genannt.

<u>Satz 215</u> Es sei L/K eine endliche Körpererweitungen. Dann sind äquivalent:

(i) L/K ist eine normale Körpererweiterung,

(ii) L ist Zerfällungskörper eines Polynoms $p \in K[X]$.

Beweis: (i) $\Rightarrow$ (ii) Nach Satz 198 (ii) gibt es $a_1,\dots,a_n \in L$, die über K algebraisch sind, derart dass $L = K(a_1,\dots,a_n)$. Für $1 \le i \le n$ besitzt das Minimalpolynom $m_{a_i,K} \in K[X]$ die Nullstelle $a_i \in L$ und ist irreduzibel über K. Daher zerfällt $m_{a_i,K}$ nach Voraussetzung über L in Linearfaktoren (für $1 \le i \le n$). Daher zerfällt auch $p := m_{a_1,K} \cdots m_{a_n,K} \in K[X]$ über L in Linearfaktoren und L ist Zerfällungskörper von p.

(ii) $\Rightarrow$ (i) Es seien $a_1,\dots,a_n \in L$ die Nullstellen von p, d.h. $p(X) = c\prod_{i=1}^{n}(X - a_i)$ für ein $c \in K$. Da L Zerfällungskörper von p ist, ist $L = K(a_1,\dots,a_n)$. Es sei nun $\overline{K}$ ein algebraischer Abschluss von K mit $L \subseteq \overline{K}$ und $\varphi : L \to \overline{K}$ ein Homomorphismus mit der Eigenschaft $\varphi(x) = x \ \forall x \in K$. Dann ist

$$p(X) = (\overline{\varphi}(p))(X) = c\prod_{i=1}^{n}(X - \varphi(a_i)) \quad (\text{mit } \overline{\varphi} : L[X] \to \overline{K}[X] \text{ wie in Lemma 204})$$

Wie im Beweis von Satz 214 folgt, dass $\varphi(a_1),\dots,\varphi(a_n)$ eine Permutation von $a_1,\dots,a_n$ sein muss. Daher ist $\varphi(a_i) \in L$ für $1 \le i \le n$ und somit

$$\varphi(L) = \varphi(K(a_1,\dots,a_n)) \subseteq K(\varphi(a_1),\dots,\varphi(a_n)) \subseteq L.$$

Da $[\varphi(L):K] = [L:K]$ muss $\varphi(L) = L$ gelten.

Beispiele: 1) $\mathbb{Q}(i)/\mathbb{Q}$ ist eine normale Körpererweiterung, da $\mathbb{Q}(i)$ Zerfällungskörper des Polynoms $X^2+1 \in \mathbb{Q}[X]$ ist.

2) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist eine normale Körpererweiterung, da $\mathbb{Q}(\sqrt{2})$ Zerfällungskörper des Polynoms $X^2 - 2 \in \mathbb{Q}[X]$ ist.

3) $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ ist eine normale Körpererweiterung, da $\mathbb{Q}(\sqrt{2}, i)$ Zerfällungskörper des Polynoms $(X^2+1)(X^2-2) \in \mathbb{Q}[X]$ ist.

4) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist keine normale Körpererweiterung. Das Polynom $X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel und besitzt in $\mathbb{Q}(\sqrt[3]{2})$ die Nullstelle $\sqrt[3]{2}$, es zerfällt über $\mathbb{Q}(\sqrt[3]{2})$ aber nicht in Linearfaktoren. (Offenbar ist

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + \sqrt[3]{2}\,b + \sqrt[3]{4}\,c \mid a,b,c \in \mathbb{Q}\} \subseteq \mathbb{R},$$

aber $X^3 - 2$ besitzt auch die beiden Nullstellen $\sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{4\pi i/3} \in \mathbb{C} \setminus \mathbb{R}$.)

Satz 216: Es sei L/K eine normale Körpererweiterung und $a, b \in L$. Dann sind äquivalent:

(i) Es gibt einen Automorphismus $\varphi : L \to L$ mit den Eigenschaften $\varphi(x) = x \ \forall x \in K$ und $\varphi(a) = b$,

(ii) $m_{a,K} = m_{b,K}$.

Beweis: (i) $\Rightarrow$ (ii) Da $m_{a,K} \in K[X]$ irreduzibel ist und die Nullstelle $a \in L$ besitzt, zerfällt es über L in Linearfaktoren, d.h.

$$m_{a,K}(X) = (X-a)(X-a_2)\dots(X-a_n) \text{ für gewisse } a_2,\dots,a_n \in L.$$

Aus $\varphi(x) = x \ \forall x \in K$ folgt

$$m_{a,K}(X) = (\overline{\varphi}(m_{a,K}))(X) = (X-\varphi(a))(X-\varphi(a_2))\dots(X-\varphi(a_n))$$
$$= (X-b)(X-\varphi(a_2))\dots(X-\varphi(a_n)),$$

d.h. b ist Nullstelle von $m_{a,K}$ und daher $m_{b,K} = m_{a,K}$

(ii) $\Rightarrow$ (i) Nach Korollar 206 gibt es einen Isomorphismus $\psi: K(a) \to K(b)$ mit den Eigenschaften $\psi(x) = x \ \forall x \in K$ und $\psi(a) = b$. Nach Satz 211 kann ψ zu einem Homomorphismus $\varphi: L \to \overline{K}$ fortgesetzt werden (wobei $\overline{K}$ einen algebraischen Abschluss von K mit $L \subseteq \overline{K}$ bezeichnet). Da L/K normal ist, folgt $\varphi(L) = L$. Daher kann man φ auch als Automorphismus $\varphi: L \to L$ mit $\varphi(x) = \psi(x) = x \ \forall x \in K$ und $\varphi(a) = \psi(a) = b$ auffassen.

Satz 217 Ist M ein Zwischenkörper der normalen Körpererweiterung L/K, so ist L/M ebenfalls eine normale Körpererweiterung.

Beweis: Es sei $\overline{K}$ ein algebraischer Abschluss von K mit der Eigenschaft $L \subseteq \overline{K}$. Dann ist $\overline{K}$ auch ein algebraischer Abschluss von M (denn auch $\overline{K}/M$ ist eine algebraische Körpererweiterung und $\overline{K}$ ist ja algebraisch abgeschlossen). Ist nun $\varphi: L \to \overline{K}$ ein Homomorphismus mit der Eigenschaft $\varphi(x) = x \ \forall x \in M$, so ist auch $\varphi(x) = x \ \forall x \in K$ und daher $\varphi(L) = L$.

Bemerkungen: 1) Es sei M ein Zwischenkörper der Körpererweiterung L/K. Daraus, dass L/K (und daher auch L/M) eine normale Körpererweiterung ist, folgt nicht, dass M/K eine normale Körpererweiterung ist. Es sei z.B. $K = \mathbb{Q}$, $L\ (\subseteq \mathbb{C})$ der Zerfällungskörper des Polynoms $X^3 - 2 \in \mathbb{Q}[X]$ und $M = \mathbb{Q}(\sqrt[3]{2})$. Dann ist L/K normal nach Satz 215 (und L/M normal nach Satz 217) aber M/K (d.h. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$) ist nicht normal.

18.1.2021

2) Jede Körpererweiterung L/K mit Grad $[L:K] = 2$ ist normal (woraus sofort die Beispiele 1) und 2) oben folgen).

Beweis: Angenommen, $p \in K[X]$ ist irreduzibel und besitzt eine Nullstelle $a \in L$. Dann ist a algebraisch über K und es gilt $2 = [L:K] = [L:K(a)] \cdot [K(a):K]$. Also ist entweder $[K(a):K] = 1$ (und daher $a \in K$) oder $[L:K(a)] = 1$ (und $L = K(a)$). Weiters muss $m_{a,K} | p$ (in $K[X]$) gelten. Da p irreduzibel ist,

$\exists c \in K\setminus\{0\}: p = c\, m_{a,K}$. Ist $a \in K$, so ist $m_{a,K}(X) = X - a$ und $p(X) = c(X-a)$, d.h. p zerfällt in Linearfaktoren. Ist $a \in L\setminus K$, so ist $\operatorname{grad} p = \operatorname{grad} m_{a,K} = 2$ und $p(X) = c\cdot m_{a,K}(X) = c(X-a)q(X)$ für ein $q \in L[X]$. Da $\operatorname{grad} m_{a,K} = 2$ und $m_{a,K}$ normiert ist, ist $q(X) = X - b$ für ein $b \in L$, d.h. $p(X) = c(X-a)(X-b)$ und p zerfällt in Linearfaktoren.

3) Es sei M ein Zwischenkörper der Körpererweiterung L/K. Daraus, dass sowohl L/M als auch M/K beides normale Körpererweiterungen sind, folgt nicht, dass L/K eine normale Körpererweiterung ist. Es sei z.B. $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt{2})$ und $L = \mathbb{Q}(\sqrt[4]{2})$. Dann ist $[M:K] = 2$ und M/K daher eine normale Körpererweiterung nach Bemerkung 2). Weiters ist $m_{\sqrt[4]{2},\mathbb{Q}(\sqrt{2})}(X) = X^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[X]$. (Dieses Polynom besitzt offenbar $\sqrt[4]{2}$ als Nullstelle und ist irreduzibles Element von $\mathbb{Q}(\sqrt{2})[X]$, da seine Nullstellen $\pm\sqrt[4]{2}$ nicht in $\mathbb{Q}(\sqrt{2})$ liegen.) Daher ist auch $[L:M] = 2$ und L/M eine normale Körpererweiterung nach Bemerkung 2). Die Körpererweiterung L/K ist aber nicht normal, denn das Polynom $p(X) = X^4 - 2 \in \mathbb{Q}[X]$ ist irreduzibel und seine Nullstelle $\sqrt[4]{2}$ liegt in $\mathbb{Q}(\sqrt[4]{2})$, es zerfällt aber über $\mathbb{Q}(\sqrt[4]{2})$ nicht in Linearfaktoren, da seine beiden Nullstellen $\pm i\sqrt[4]{2}$ nicht in $\mathbb{Q}(\sqrt[4]{2})$ $(\subseteq \mathbb{R})$ liegen.

Definition: Es sei L/K eine algebraische Körpererweiterung und $\overline{K}$ ein algebraischer Abschluss von K. Als Separabilitätsgrad $[L:K]_s$ bezeichnet man

$$[L:K]_s := \left|\{\varphi : L \to \overline{K} \mid \varphi \text{ ist Homomorphismus und } \varphi(x) = x \ \forall x \in K\}\right|.$$

Bemerkung: Ist $\tilde{K}$ ein weiterer algebraischer Abschluss von K, so gibt es nach Korollar 213 einen Isomorphismus $\psi : \overline{K} \to \tilde{K}$ mit der Eigenschaft $\psi(x) = x \ \forall x \in K$. Bezeichnet

$\overline{E} := \{\varphi : L \to \overline{K} \mid \varphi$ ist Homomorphismus und $\varphi(x) = x \ \forall x \in K\}$ und

$\tilde{E} := \{\varphi : L \to \tilde{K} \mid \varphi$ ist Homomorphismus und $\varphi(x) = x \ \forall x \in K\}$, so ist

$f : \overline{E} \to \tilde{E}$, $f(\varphi) = \psi \circ \varphi$ eine bijektive Abbildung, da $g : \tilde{E} \to \overline{E}$, $g(\varphi) = \psi^{-1}\circ\varphi$ die Bedingungen $g\circ f = id_{\overline{E}}$ und $f\circ g = id_{\tilde{E}}$ erfüllt. D.h. die Größe $[L:K]_s$ hängt nicht von der Wahl von $\overline{K}$ ab und ist daher wohldefiniert.

Satz 218 Es sei L/K eine algebraische Körpererweiterung und $a \in L$. Dann ist $[K(a):K]_s$ die Anzahl der verschiedenen Nullstellen von $m_{a,K}$ in einem algebraischen Abschluss $\overline{K}$ von K.

Beweis: Es sei $\varphi: K(a) \to \overline{K}$ ein Homomorphismus mit der Eigenschaft $\varphi(x)=x \ \forall x \in K$. Ist $n = \operatorname{grad} m_{a,K}$, so ist $K(a) = \left\{ \sum_{i=0}^{n-1} x_i a^i \,\middle|\, x_0, x_1, \dots, x_{n-1} \in K \right\}$. Ist $m_{a,K}(X) = \sum_{i=0}^{n} b_i X^i$, so ist $0 = m_{a,K}(a) = \sum_{i=0}^{n} b_i a^i$ und daher

$$0 = \varphi(0) = \varphi\left(\sum_{i=0}^{n} b_i a^i\right) = \sum_{i=0}^{n} b_i \varphi(a)^i = m_{a,K}(\varphi(a)),$$

d.h. $\varphi(a) \in \overline{K}$ ist Nullstelle von $m_{a,K}$ und $\varphi: K(a) \to \overline{K}$ hat die Gestalt

$\varphi\left(\sum_{i=0}^{n-1} x_i a^i\right) = \sum_{i=0}^{n-1} x_i b^i$, wobei $b \in \overline{K}$ eine Nullstelle von $m_{a,K}$ ist. Da dabei $\varphi(a) = b$ ist, erhält man für verschiedene Nullstellen b von $m_{a,K}$ auch verschiedene Abbildungen. Nach dem Beweis von Satz 205 ist ein derartiges φ tatsächlich ein Homomorphismus (und erfüllt $\varphi(x)=x \ \forall x \in K$).

Korollar 219: Es sei L/K eine normale Körpererweiterung. Dann ist

$[L:K]_s = |\{\varphi: L \to L \mid \varphi \text{ ist ein Automorphismus und } \varphi(x)=x \ \forall x \in K\}|$.

Beweis: Ist $\varphi: L \to \overline{K}$ ein Homomorphismus mit der Eigenschaft $\varphi(x)=x \ \forall x \in K$, so gilt (wegen Satz 214) $\varphi(L) = L$, d.h. φ kann als Automorphismus von L aufgefasst werden.

Lemma 220: Es sei L/K eine algebraische Körpererweiterung, A ein algebraisch abgeschlossener Körper und $\varphi: K \to A$ ein Homomorphismus, so gibt es genau $[L:K]_s$ Homomorphismen $\psi: L \to A$, die φ fortsetzen (d.h. $\psi(x) = \varphi(x) \ \forall x \in K$).

Beweis: Es sei $\overline{K}$ ein algebraischer Abschluss von K mit der Eigenschaft $L \subseteq \overline{K}$. Weiters enthält A einen algebraischen Abschluss von $\varphi(K)$, der nach Korollar 212 zu $\overline{K}$ isomorph ist. Wir können daher oBdA annehmen, dass A algebraischer Abschluss von $\varphi(K)$ ist. Nach Korollar 212 gibt es einen Isomorphismus $\overline{\varphi}: \overline{K} \to A$, der φ fortsetzt (d.h. $\overline{\varphi}(x) = \varphi(x) \ \forall x \in K$). Es seien nun

$E = \{\psi: L \to \overline{K} \mid \psi \text{ ist Homomorphismus und } \psi(x) = x \ \forall x \in K\}$ und

$F = \{\psi: L \to A \mid \psi \text{ ist Homomorphismus und } \psi(x) = \varphi(x) \ \forall x \in K\}$.

Dann ist $|F| = |E| = [L:K]_s$, da die Abbildung $f: E \to F$, $f(\psi) = \overline{\varphi} \circ \psi$ bijektiv ist. (Setzt man $g: F \to E$, $g(\psi) = \overline{\varphi}^{-1} \circ \psi$, so sind die Relationen $g \circ f = \mathrm{id}_E$ und $f \circ g = \mathrm{id}_F$ erfüllt.)

Satz 221 (i) Ist L/K eine algebraische Körpererweiterung und M ein Zwischenkörper, so gilt $[L:K]_s = [L:M]_s \cdot [M:K]_s$.

(ii) Ist L/K eine endliche Körpererweiterung, so ist $[L:K]_s \leq [L:K]$.

Beweis: (i) Nach Satz 199 sind L/M und M/K beides algebraische Körpererweiterungen. Es sei $\overline{K}$ ein algebraischer Abschluss von K mit der Eigenschaft $L \subseteq \overline{K}$. Es gibt (nach Definition) genau $[M:K]_s$ Homomorphismen $\varphi : M \to \overline{K}$ mit der Eigenschaft $\varphi(x) = x \ \forall x \in K$. Nach Lemma 220 gibt es für jede dieser Abbildungen genau $[L:M]_s$ Homomorphismen $\psi : L \to \overline{K}$, die das jeweilige φ fortsetzen (und daher $\psi(x) = x \ \forall x \in K$ erfüllen). Man erhält auf diese Weise $[L:M]_s \cdot [M:K]_s$ verschiedene Homomorphismen $\psi : L \to \overline{K}$ mit der Eigenschaft $\psi(x) = x \ \forall x \in K$. Nun ist aber jeder Homomorphismus $\psi : L \to \overline{K}$, der $\psi(x) = x \ \forall x \in K$ erfüllt, die Fortsetzung eines Homomorphismus $\varphi : M \to \overline{K}$, der $\varphi(x) = x \ \forall x \in K$ erfüllt. (Man kann ja als φ die Einschränkung von ψ auf M wählen.) Daher haben wir bereits alle solchen Homomorphismen gefunden und es gilt $[L:K]_s = [L:M]_s \cdot [M:K]_s$.

(ii) Die Behauptung gilt für algebraische Körpererweiterungen der Gestalt $K(a)/K$ (d.h. $[K(a):K]_s \leq [K(a):K]$), da $[K(a):K]_s$ nach Satz 218 die Anzahl der verschiedenen Nullstellen von $m_{a,K}$ ist und $[K(a):K] = \operatorname{grad} m_{a,K}$ nach Satz 197 (iii).

Nach Satz 198 (ii) gibt es $a_1, \dots, a_n \in L$, die algebraisch über K sind, derart dass $L = K(a_1, \dots, a_n)$. Daraus folgt nun

$$\begin{aligned}
[L:K]_s = [K(a_1,\dots,a_n):K]_s &\overset{(i)}{=} \prod_{i=1}^{n} [K(a_1,\dots,a_i):K(a_1,\dots,a_{i-1})]_s \\
&= \prod_{i=1}^{n} [K(a_1,\dots,a_{i-1})(a_i):K(a_1,\dots,a_{i-1})]_s \\
&\leq \prod_{i=1}^{n} [K(a_1,\dots,a_{i-1})(a_i):K(a_1,\dots,a_{i-1})] \\
&= \prod_{i=1}^{n} [K(a_1,\dots,a_i):K(a_1,\dots,a_{i-1})] \\
&= [K(a_1,\dots,a_n):K] = [L:K]
\end{aligned}$$

Korollar 222 Es sei M ein Zwischenkörper der endlichen Körpererweiterung L/K. Dann sind äquivalent:

(i) $[L:K]_s = [L:K]$,

(ii) $[L:M]_s = [L:M]$ und $[M:K]_s = [M:K]$.

Beweis: Folgt sofort aus Satz 221.

Definition: Es sei K ein Körper und $p \in K[X]$. Ist p irreduzibel, so wird p separabel genannt, wenn es (in einem algebraischen Abschluss $\overline{K}$ von K) keine mehrfachen Nullstellen besitzt. Ist $\operatorname{grad} p \geq 1$, so wird p separabel genannt, wenn jeder seiner irreduziblen Faktoren separabel ist.

Lemma 223 Es sei K ein Körper und $p \in K[X]$ irreduzibel.

(i) p ist separabel $\Longleftrightarrow$ $p' \neq 0$,

(ii) Besitzt p eine mehrfache Nullstelle, so ist $\operatorname{char} K > 0$.

Beweis: (i) Folgt sofort aus Korollar 176 (ii).

(ii) Ist $\operatorname{char} K = 0$, so gilt $\operatorname{grad} p' = \operatorname{grad} p - 1 \geq 0$ (nach Lemma 174 (iii)). Daher ist $p' \neq 0$ und p ist separabel nach (i).

Bsp.: Es sei $K = \mathbb{Z}_2(T)$ (wobei T eine Unbestimmte ist) und $p(X) = X^2 - T \in K[X]$. Nach dem Eisensteinkriterium (Satz 185) ist p irreduzibel. (Zunächst ist $T \in \mathbb{Z}_2[T]$ irreduzibel in $\mathbb{Z}_2[T]$ nach Lemma 177 (ii). Daher ist T nach Satz 183 auch irreduzibel als Element von $\mathbb{Z}_2[T][X]$. Da $T \mid T$, $T \mid 0$, $T \nmid 1$ und $T^2 \nmid T$ gelten, ist p irreduzibel in $K[X] = \mathbb{Z}_2(T)[X]$.) Da $p'(X) = 2X = 0$, besitzt p wegen Lemma 223 (i) eine mehrfache Nullstelle in $\overline{K}$.

Definition: Es sei K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und $a \in \overline{K}$. Dann heißt a separabel über K, wenn $m_{a,K}$ separabel ist.

Korollar 224 Es sei K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und $a \in \overline{K}$. Dann sind äquivalent:

(i) a ist separabel,

(ii) $m_{a,K}' \neq 0$.

Beweis: Folgt sofort aus Lemma 223 (i).

Definition: Eine algebraische Körpererweiterung L/K heißt separabel, wenn alle $a \in L$ separabel über K sind.

Satz 225: Es sei L/K eine endliche Körpererweiterung. Dann sind äquivalent:

(i) Die Körpererweiterung L/K ist separabel,

(ii) Es gibt $a_1, \dots, a_n \in L$, die alle über K separabel sind, derart dass $L = K(a_1, \dots, a_n)$,

(iii) $[L:K]_s = [L:K]$.

<u>Beweis</u>: (i) $\Rightarrow$ (ii) Nach Satz 198 (ii) gibt es $a_1, \dots, a_n \in L$, derart dass $L = K(a_1, \dots, a_n)$. Nach Voraussetzung sind $a_1, \dots, a_n$ separabel über K.

(ii) $\Rightarrow$ (iii) Für $1 \leq i \leq n$ ist $m_{a_i,K} \in K[X]$ separabel über K und besitzt daher nur einfache Nullstellen. Fasst man $m_{a_i,K}$ als Element von $K(a_1, \dots, a_{i-1})[X]$ auf, braucht es nicht mehr irreduzibel zu sein; nach Satz 195 (iii) gilt allerdings $m_{a_i,K(a_1,\dots,a_{i-1})} \mid m_{a_i,K}$ (im Polynomring $K(a_1, \dots, a_{i-1})[X]$). Daher besitzt auch $m_{a_i,K(a_1,\dots,a_{i-1})}$ nur einfache Nullstellen und a_i ist auch separabel über $K(a_1, \dots, a_{i-1})$.

Daher stimmen

$$\operatorname{grad} m_{a_i,K(a_1,\dots,a_{i-1})} = [K(a_1,\dots,a_{i-1})(a_i) : K(a_1,\dots,a_{i-1})] = [K(a_1,\dots,a_i) : K(a_1,\dots,a_{i-1})]$$

und die Anzahl der (paarweise verschiedenen) Nullstellen von $m_{a_i,K(a_1,\dots,a_{i-1})}$, d.h.

$$[K(a_1,\dots,a_{i-1})(a_i) : K(a_1,\dots,a_{i-1})]_s = [K(a_1,\dots,a_i) : K(a_1,\dots,a_{i-1})]_s,$$

nach Satz 218 überein. Daraus folgt

$$[L:K]_s = [K(a_1,\dots,a_n):K]_s \overset{\text{Satz 221 (i)}}{=} \prod_{i=1}^{n} [K(a_1,\dots,a_i) : K(a_1,\dots,a_{i-1})]_s$$

$$= \prod_{i=1}^{n} [K(a_1,\dots,a_i) : K(a_1,\dots,a_{i-1})] = [K(a_1,\dots,a_n):K] = [L:K].$$

(iii) $\Rightarrow$ (i) Ist $a \in L$, so folgt aus Korollar 222, dass $[K(a):K]_s = [K(a):K]$. D.h. die Anzahl der Nullstellen von $m_{a,K}$ stimmt mit $\operatorname{grad} m_{a,K}$ überein (wegen Satz 218 bzw. Satz 197 (iii)). Daher besitzt $m_{a,K}$ keine mehrfachen Nullstellen und ist daher separabel über K. D.h. a ist separabel über K.

<u>Korollar 226</u>: Ist die endliche Körpererweiterung L/K normal und separabel, so ist $[L:K] = |\{\varphi : L \to L \mid \varphi \text{ ist Automorphismus und } \varphi(x) = x \ \forall x \in K\}|$.

<u>Beweis</u>: Folgt sofort aus Satz 225 und Korollar 219.

<u>Korollar 227</u>: Ist K ein Körper mit $\operatorname{char} K = 0$, so ist jede algebraische Körpererweiterung L/K separabel.

<u>Beweis</u>: Ist $a \in L$, so ist $m_{a,K} \in K[X]$ separabel wegen Lemma 223 (ii)

<u>Korollar 228</u>: Es sei L/K eine endliche Körpererweiterung und M ein Zwischenkörper. Dann sind äquivalent:

(i) L/K ist separabel,

(ii) L/M und M/K sind beide separabel.

<u>Beweis</u>: Folgt sofort aus Korollar 222 und Satz 225.

Satz 229 (Satz vom primitiven Element) Es sei L/K eine endliche Körpererweiterung.

(i) Ist K ein endlicher Körper, so ist die Körpererweiterung L/K einfach, d.h. $\exists a \in L : L = K(a)$,

(ii) Ist L/K eine separable Körpererweiterung, so ist L/K einfach, d.h. $\exists a \in L : L = K(a)$.

Beweis: (i) Da $|L| = |K|^{[L:K]}$ ist auch L ein endlicher Körper. Nach Korollar 191 ist $(L^*, \cdot)$ eine zyklische Gruppe. Ist $a \in L^*$ ein erzeugendes Element, so ist $L = L^* \cup \{0\} = \{1, a, a^2, \dots, a^{|L|-2}\} \cup \{0\} = K(a)$.

(ii) Wegen (i) können wir voraussetzen, dass K unendlich ist.

Wir zeigen zunächst: Ist $L = K(b, c)$ für gewisse $b, c \in L$, so $\exists a \in L : L = K(a)$.

Da L/K separabel ist, gilt nach Satz 225 $[L:K]_s = [L:K] = n$.

D.h. es gibt genau n Homomorphismen $\varphi_1, \dots, \varphi_n : L \to \overline{K}$ mit der Eigenschaft $\varphi_i(x) = x \quad \forall x \in K \ \forall i \in \{1, \dots, n\}$ (wobei $\overline{K}$ einen algebraischen Abschluss von K bezeichnet). Es sei

$$p(X) = \prod_{1 \leq i < j \leq n} \left((\varphi_i(b) - \varphi_j(b)) X + \varphi_i(c) - \varphi_j(c) \right) \in \overline{K}[X].$$

Für $i, j \in \{1, \dots, n\}, i \neq j$ ist $\varphi_i \neq \varphi_j$. Daher muss $\varphi_i(b) \neq \varphi_j(b)$ oder $\varphi_i(c) \neq \varphi_j(c)$ gelten. Das impliziert $p \neq 0$. Da K unendlich ist $\exists \lambda \in K : p(\lambda) \neq 0$.

Daraus folgt $\lambda \varphi_i(b) - \lambda \varphi_j(b) \neq \varphi_j(c) - \varphi_i(c)$ und daher

$$\varphi_i(\lambda b + c) = \lambda \varphi_i(b) + \varphi_i(c) \neq \lambda \varphi_j(b) + \varphi_j(c) = \varphi_j(\lambda b + c) \quad \text{für } 1 \leq i < j \leq n.$$

Setzt man $a := \lambda b + c$, so sind $\varphi_1(a), \dots, \varphi_n(a)$ daher paarweise verschieden und alle Nullstellen von $m_{a,K}$. (Aus $0 = m_{a,K}(a)$ folgt ja $0 = \varphi_i(0) = \varphi_i(m_{a,K}(a)) = m_{a,K}(\varphi_i(a))$.) Daraus folgt

$$[K(a):K] = \operatorname{grad} m_{a,K} \geq n = [L:K] = [L:K(a)] \cdot [K(a):K] \geq [K(a):K]$$

Das ist nur möglich wenn $[L:K] = [K(a):K]$ und daher $[L:K(a)] = 1$, d.h. $L = K(a)$.

Wir behandeln nun den allgemeinen Fall. Nach Satz 198 (ii) gibt es $b_1, \dots, b_m \in L : L = K(b_1, \dots, b_m)$. Wir verwenden Induktion nach m.

Für $m = 1$ ist nichts zu beweisen und der Fall $m = 2$ wurde schon bewiesen.

Es sei die Behauptung für m schon bewiesen, d.h. $\exists c \in L : K(b_1, \dots, b_m) = K(c)$.

Dann gibt es nach dem Fall $m = 2$ ein $a \in L$, derart dass $K(c, b_{m+1}) = K(a)$ und daher

$$K(b_1, \dots, b_{m+1}) = K(b_1, \dots, b_m)(b_{m+1}) = K(c)(b_{m+1}) = K(c, b_{m+1}) = K(a).$$

21.1.2021

Bsp.: Gesucht ist ein primitives Element für die Körpererweiterung $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.
Wir betrachten zunächst die Körpererweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Wir wissen, dass $m_{\sqrt{2},\mathbb{Q}}(x) = x^2-2$ und $m_{\sqrt{2},\mathbb{Q}}$ besitzt die beiden Nullstellen $\pm\sqrt{2}$. Es gibt $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]_s = [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ Einbettungen $\varphi_1,\varphi_2 : \mathbb{Q}(\sqrt{2}) \hookrightarrow \overline{\mathbb{Q}}$ mit der Eigenschaft $\varphi_i(x) = x \;\forall x\in\mathbb{Q}$, wobei $\varphi_1(\sqrt{2}) = \sqrt{2}$ und $\varphi_2(\sqrt{2}) = -\sqrt{2}$ gelten soll, dh $\varphi_1(a+b\sqrt{2}) = a + b\varphi_1(\sqrt{2}) = a+b\sqrt{2}$ und $\varphi_2(a+b\sqrt{2}) = a+b\varphi_2(\sqrt{2}) = a-b\sqrt{2}$ (mit $a,b\in\mathbb{Q}$).
Wir betrachten nun die Körpererweiterung $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}(\sqrt{2})$, dh $\mathbb{Q}(\sqrt{2})(\sqrt{3})/\mathbb{Q}(\sqrt{2})$.
Es ist $m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(x) = x^2-3$ und $m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}$ besitzt die beiden Nullstellen $\pm\sqrt{3}$.
Für $i\in\{1,2\}$ gibt es nun $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]_s = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$ Einbettungen $\psi_j : \mathbb{Q}(\sqrt{2},\sqrt{3}) \hookrightarrow \overline{\mathbb{Q}}$, die φ_i fortsetzen. Dabei setzen
$\psi_1(\alpha+\beta\sqrt{3}) = \varphi_1(\alpha)+\varphi_1(\beta)\sqrt{3} = \alpha+\beta\sqrt{3}$, $\psi_2(\alpha+\beta\sqrt{3}) = \varphi_1(\alpha)+\varphi_1(\beta)(-\sqrt{3}) = \alpha-\beta\sqrt{3}$
die Einbettung $\varphi_1 : \mathbb{Q}(\sqrt{2}) \hookrightarrow \overline{\mathbb{Q}}$ fort und
$\psi_3(\alpha+\beta\sqrt{3}) = \varphi_2(\alpha)+\varphi_2(\beta)\sqrt{3}$ und $\psi_4(\alpha+\beta\sqrt{3}) = \varphi_2(\alpha)-\varphi_2(\beta)\sqrt{3}$
die Einbettung $\varphi_2 : \mathbb{Q}(\sqrt{2}) \hookrightarrow \overline{\mathbb{Q}}$ fort (jeweils mit $\alpha,\beta\in\mathbb{Q}(\sqrt{2})$).
Dh die vier Einbettungen haben folgende Gestalt (mit $a,b,c,d\in\mathbb{Q}$):

$$\psi_1(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \quad (\text{dh } \psi_1 = \mathrm{id}_{\mathbb{Q}(\sqrt{2},\sqrt{3})})$$
$$\psi_2(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$$
$$\psi_3(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$$
$$\psi_4(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6} \quad (\text{dh } \psi_4 = \psi_3\circ\psi_2)$$

(Da $1,\sqrt{2}$ eine Basis von $\mathbb{Q}(\sqrt{2})$ als $\mathbb{Q}$-Vektorraum ist und $1,\sqrt{3}$ eine Basis von $\mathbb{Q}(\sqrt{2},\sqrt{3})$ als $\mathbb{Q}(\sqrt{2})$-Vektorraum, ist $1\cdot 1, \sqrt{2}\cdot 1, 1\cdot\sqrt{3}, \sqrt{2}\cdot\sqrt{3}$ (dh $1,\sqrt{2},\sqrt{3},\sqrt{6}$) eine Basis von $\mathbb{Q}(\sqrt{2},\sqrt{3})$ als $\mathbb{Q}$-Vektorraum.)
Für $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$ sind $\psi_1(\sqrt{2}+\sqrt{3}) = \sqrt{2}+\sqrt{3}$, $\psi_2(\sqrt{2}+\sqrt{3}) = \sqrt{2}-\sqrt{3}$, $\psi_3(\sqrt{2}+\sqrt{3}) = -\sqrt{2}+\sqrt{3}$ und $\psi_4(\sqrt{2}+\sqrt{3}) = -\sqrt{2}-\sqrt{3}$ paarweise verschieden.
Dh sind im Beweis von Satz 229 (ii) $K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$, $b=\sqrt{2}$ und $c=\sqrt{3}$, so kann man $\lambda=1$ wählen. Dann ist $a=\sqrt{2}+\sqrt{3}$ und $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Definition: Es sei K ein Körper. Dann bezeichne $\mathrm{Aut}\,K$ die Gruppe der Automorphismen von K, dh $\mathrm{Aut}\,K = \{\sigma : K\to K \mid \sigma \text{ ist Automorphismus}\}$.

Definition: Eine algebraische Körpererweiterung L/K heißt galoissch oder Galoiserweiterung wenn sie normal und separabel ist. Ist L/K eine Galoiserweiterung, so definiert man die Galoisgruppe $G(L/K)$ durch $G(L/K) = \{\sigma\in\mathrm{Aut}\,L \mid \sigma(x) = x \;\forall x\in K\}$.

Bemerkungen: 1) Aus den Lemmata 65 und 66 folgt sofort, dass Aut K tatsächlich eine Gruppe ist (und $G(L/K)$ ist Untergruppe von Aut L).
2) Ist L/K eine endliche Galoiserweiterung, so gilt $|G(L/K)| = [L:K]$ nach Korollar 226.

Lemma 230: Es sei L/K eine Galoiserweiterung und $p \in K[X]$ irreduzibel. Besitzt p eine Nullstelle in L, so operiert $G(L/K)$ transitiv auf der Menge der Nullstellen von p. (D.h. sind $a, b \in L$ beide Nullstellen von p, so gibt es ein $\sigma \in G(L/K)$ mit der Eigenschaft $\sigma(a) = b$.)

Beweis: Es sei $a \in L$ Nullstelle von p. Da L/K eine normale Körpererweiterung ist, zerfällt p über L in Linearfaktoren, d.h. es gibt $c \in K$ und $a_1 = a, a_2, \dots, a_n \in L$, derart dass $p(X) = c(X-a_1)\dots(X-a_n)$. (Daraus folgt wegen Korollar 196 sofort $m_{a_i,K}(X) = (X-a_1)\dots(X-a_n)$ für $1 \leq i \leq n$.) Ist $\sigma \in G(L/K)$, so gilt wegen $p(X) = p^\sigma(X) = c(X-\sigma(a_1))\dots(X-\sigma(a_n))$, dass $\sigma(a_1), \dots, \sigma(a_n)$ eine Permutation von $a_1, \dots, a_n$ ist. Insbesondere ist $\sigma(a_i)$ eine Nullstelle von p für $1 \leq i \leq n$ und $G(L/K)$ operiert auf der Menge $\{a_1, \dots, a_n\}$ der Nullstellen von p (denn $id_L(a_i) = a_i$ für $1 \leq i \leq n$ und $(\sigma \circ \tau)(a_i) = \sigma(\tau(a_i))$ für $\sigma, \tau \in G(L/K)$ und $1 \leq i \leq n$). Nach Satz 216 gibt es für $1 \leq i, j \leq n$ ein $\sigma \in G(L/K)$ mit der Eigenschaft $\sigma(a_i) = a_j$, d.h. $G(L/K)$ operiert transitiv auf $\{a_1, \dots, a_n\}$.

Beispiele: 1) $\mathbb{Q}(i)/\mathbb{Q}$ ist eine Galoiserweiterung ($\mathbb{Q}(i)/\mathbb{Q}$ ist normal, da $\mathbb{Q}(i)$ Zerfällungskörper von $X^2+1 \in \mathbb{Q}[X]$ ist und seperabel, da char $\mathbb{Q} = 0$). Es ist $G(\mathbb{Q}(i)/\mathbb{Q}) = \{id_{\mathbb{Q}(i)}, \sigma\}$, wobei $\sigma: \mathbb{Q}(i) \to \mathbb{Q}(i)$ die komplexe Konjugation bezeichnet (d.h. $\sigma(x+iy) = x-iy$ für $x, y \in \mathbb{Q}$).
2) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist eine Galoiserweiterung ($\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ist normal, da $\mathbb{Q}(\sqrt{2})$ Zerfällungskörper von $X^2-2 \in \mathbb{Q}[X]$ ist und seperabel, da char $\mathbb{Q} = 0$). Es ist $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id_{\mathbb{Q}(\sqrt{2})}, \sigma\}$, wobei $\sigma: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ die Abbildung $\sigma(x+y\sqrt{2}) = x-y\sqrt{2}$ (mit $x, y \in \mathbb{Q}$) bezeichnet.
3) $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ ist eine Galoiserweiterung ($\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ ist normal, da $\mathbb{Q}(\sqrt{2},\sqrt{3})$ Zerfällungskörper von $(X^2-2)(X^2-3)$ ist und seperabel, da char $\mathbb{Q} = 0$). Es ist $G(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \{\psi_1, \psi_2, \psi_3, \psi_4\}$, wobei $\psi_1, \psi_2, \psi_3, \psi_4$ die selbe Bedeutung wie im Bsp. nach Satz 229 haben sollen. (Es ist offensichtlich, dass ψ_i als Element von Aut $\mathbb{Q}(\sqrt{2},\sqrt{3})$ aufgefasst werden kann und dass $\psi_i(x) = x \; \forall x \in \mathbb{Q}$.) Da $\psi_i^2 = id_{\mathbb{Q}(\sqrt{2},\sqrt{3})}$ für $1 \leq i \leq 4$ ist $(G(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}), \circ) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

Lemma 231: Es sei L ein Körper und $G \leq \operatorname{Aut} L$. Dann ist $K := \{a \in L \mid \sigma(a) = a \ \forall \sigma \in G\}$ ein Teilkörper von L.

Beweis: Es ist $K \neq \emptyset$, da $0, 1 \in K$. Sind $a, b \in K$, so gelten $\sigma(a-b) = \sigma(a) - \sigma(b) = a - b \ \forall \sigma \in G$ und $\sigma(ab) = \sigma(a)\sigma(b) = ab \ \forall \sigma \in G$, d.h. $a-b, ab \in K$. Damit ist gezeigt, dass K ein Unterring von L ist. Ist $a \in K \setminus \{0\}$, so ist $\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1} \ \forall \sigma \in G$ und daher $a^{-1} \in K$. D.h. K ist ein Teilkörper von L.

Definition: Es sei K ein Körper und $G \leq \operatorname{Aut} K$. Dann bezeichnet man $K^G := \{a \in K \mid \sigma(a) = a \ \forall \sigma \in G\}$ als Fixkörper von G.

Satz 232: Es sei L/K eine algebraische Körpererweiterung und G die Gruppe $G = \{\sigma \in \operatorname{Aut} L \mid \sigma(a) = a \ \forall a \in K\}$. Dann sind äquivalent:

(i) L/K ist eine Galoiserweiterung,

(ii) $L^G = K$.

Beweis: (i) $\Rightarrow$ (ii) Ist $a \in K$, so ist nach Definition $\sigma(a) = a \ \forall \sigma \in G$, d.h. $K \subseteq L^G$. Ist $a \in L \setminus K$, so ist $\operatorname{grad} m_{a,K} \geq 2$. Da L/K normal ist, zerfällt $m_{a,K}$ über L in Linearfaktoren. Da L/K separabel ist, hat a Vielfachheit 1 als Nullstelle von $m_{a,K}$. Daher gibt es ein $b \in L \setminus \{a\}$ mit $m_{a,K}(b) = 0$ (und folglich $m_{b,K} = m_{a,K}$). Nach Satz 216 gibt es ein $\sigma \in G$ mit der Eigenschaft $\sigma(a) = b$, d.h. $a \notin L^G$. Also gilt $K = L^G$.

(ii) $\Rightarrow$ (i) Es sei $a \in L$ und $a_1 = a, a_2, \dots, a_n \in L$ die (paarweise verschiedenen) Nullstellen von $m_{a,K}$ in L. Wegen Satz 168 (ii) ist $n \leq \operatorname{grad} m_{a,K}$. Ist $\sigma \in G$, so permutiert σ die Nullstellen von $m_{a,K}$. Es sei nun

$$p(X) := \prod_{i=1}^{n} (X - a_i) = \sum_{j=0}^{n} b_j X^j \in L[X].$$

Da σ die Nullstellen von p permutiert ist $p^\sigma = p$ und daher $b_j \in L^G = K$ für $0 \leq j \leq n$, also $p \in K[X]$. Da $p(a) = p(a_1) = 0$ folgt aus Satz 195 (iii), dass $m_{a,K} \mid p$ (in $K[X]$). Weil $\operatorname{grad} p = n \leq \operatorname{grad} m_{a,K}$ muss aber $p = m_{a,K}$ gelten. Daher zerfällt $m_{a,K}$ über L in Linearfaktoren und ist separabel. Da $a \in L$ beliebig war, ist die Körpererweiterung L/K separabel. Ist $p \in K[X]$ irreduzibel (und oBdA normiert) und besitzt eine Nullstelle $a \in L$, so ist $p = m_{a,K}$ und p zerfällt nach dem obigen Argument in Linearfaktoren, d.h. die Körpererweiterung L/K ist normal.

25.1.2021

Bemerkung: Satz 232 enthält die folgende Aussage: Ist L/K eine Galoiserweiterung, so gilt $L^{G(L/K)} = K$.

Beispiel: Die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist algebraisch aber keine Galoiserweiterung, da sie nicht normal ist. Ist $\sigma \in G$ mit $G = \{\sigma \in \operatorname{Aut} \mathbb{Q}(\sqrt[3]{2}) \mid \sigma(a) = a \; \forall a \in \mathbb{Q}\}$, so muss $\sigma(\sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2})$ eine Nullstelle von $X^3 - 2 \in \mathbb{Q}[X]$ sein. Da $\sqrt[3]{2}$ die einzige Nullstelle von X^3-2 in $\mathbb{Q}(\sqrt[3]{2})$ ist, muss $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ gelten, woraus $\sigma = id_{\mathbb{Q}(\sqrt[3]{2})}$ folgt.
Also ist $G = \{id_{\mathbb{Q}(\sqrt[3]{2})}\}$ und daher $\mathbb{Q}(\sqrt[3]{2})^G = \mathbb{Q}(\sqrt[3]{2}) \supsetneqq \mathbb{Q}$.
(D.h. in diesem Beispiel ist $K \subsetneqq L^G$. Die Beziehung $K \subseteq L^G$ gilt allgemein und kann nicht verletzt sein.)

Satz 233: Es sei L ein Körper und H eine endliche Untergruppe von $\operatorname{Aut} L$. Dann gelten:

(i) L/L^H ist eine Galoiserweiterung,
(ii) $[L:L^H] = |H|$,
(iii) $G(L/L^H) = H$

Beweis: (i) Für $a \in L$ sei $\Sigma_a := \{\sigma(a) \mid \sigma \in H\} (\subseteq L)$. Da H endlich ist, ist auch Σ_a endlich. Ist $\Sigma_a = \{a_1, \dots, a_n\}$ (mit $a_1 = a$), so ist $n = |\Sigma_a| \leq |H|$. Die Gruppe H operiert auf Σ_a. (Ist $b \in \Sigma_a$, so $\exists \sigma \in H: b = \sigma(a)$. Für $\tau \in H$ ist nun $\tau(b) = \underbrace{(\tau \circ \sigma)}_{\in H}(a) \in \Sigma_a$.)

D.h. $\sigma \in H$ permutiert $a_1, \dots, a_n$. Es sei $p_a(X) := \prod_{i=1}^{n} (X - a_i)$. Dann gilt $p_a^\sigma = p_a \; \forall \sigma \in H$ und daher $p_a \in L^H[X]$. Da $p_a(a) = p_a(a_1) = 0$, ist a algebraisch über L^H. Das Polynom p_a ist separabel über L^H. Da (im Polynomring $L^H[X]$) die Relation $m_{a,L^H} \mid p_a$ gelten muss, ist auch m_{a,L^H} separabel über L^H, d.h. a ist separabel über L^H. Da $a \in L$ beliebig war, ist damit gezeigt, dass die Körpererweiterung L/L^H algebraisch und separabel ist. Ist $p \in L^H[X]$ irreduzibel (und o.B.d.A. normiert) und besitzt eine Nullstelle $a \in L$, so ist $p = m_{a,L^H}$ und wegen $m_{a,L^H} \mid p_a$ (d.h. $p \mid p_a$) zerfällt p über L in Linearfaktoren. D.h. die Körpererweiterung L/L^H ist auch normal. Damit ist gezeigt, dass L/L^H eine Galoiserweiterung ist.

(ii) und (iii) Nach dem Beweis von (i) gilt $\operatorname{grad} m_{a,L^H} \leq \operatorname{grad} p_a \leq |H| \; \forall a \in L$.
Angenommen, es wäre $|H| < [L:L^H]$. Dann gäbe es einen Zwischenkörper M der Körpererweiterung L/L^H, derart dass $|H| < [M:L^H] < \infty$. (Wähle $c_1 \in L \setminus L^H$. Ist $|H| < [L^H(c_1):L^H]$, so fertig. Falls nicht, wähle $c_2 \in L \setminus L^H(c_1)$. Verfahre weiter so, d.h. sind $c_1, \dots, c_n \in L$ schon gewählt und $[L^H(c_1, \dots, c_n):L^H] \leq |H|$, so wähle

$c_{n+1} \in L \setminus L^H(c_1,\dots,c_n)$. Wegen

$$[L^H(c_1):L^H] < [L^H(c_1,c_2):L^H] < [L^H(c_1,c_2,c_3):L^H] < \dots < \infty$$

muss es ein $n \geq 1$ mit der Eigenschaft $[L^H(c_1,\dots,c_n):L^H] > |H|$ geben.
Setze $M := L^H(c_1,\dots,c_n)$.) Nach Korollar 228 ist die Körpererweiterung M/L^H separabel. Nach Satz 229 (Satz vom primitiven Element) $\exists c \in M : M = L^H(c)$.
Aus Satz 197 (iii) folgt $\operatorname{grad} m_{c,L^H} = [L^H(c):L^H] = [M:L^H] > |H|$, ein Widerspruch. Also ist $[L:L^H] \leq |H| < \infty$. Nun ist H eine Untergruppe von $\{\sigma \in \operatorname{Aut} L \mid \sigma(x) = x \ \forall x \in L^H\} = G(L/L^H)$ und daher $|H| \leq |G(L/L^H)| \overset{\text{Kor. 226}}{=} [L:L^H]$.
Also ist $|H| = [L:L^H] = |G(L/L^H)|$ und daher $H = G(L/L^H)$ (da H eine endliche Untergruppe von $G(L/L^H)$ ist).

<u>Lemma 234</u> Es sei L/K eine Galoiserweiterung.

(i) Ist M ein Zwischenkörper der Körpererweiterung L/K, so ist L/M ebenfalls eine Galoiserweiterung,

(ii) Sind M_1 und M_2 zwei Zwischenkörper der Körpererweiterung L/K und $M_1 \subseteq M_2$, so gilt $G(L/M_2) \leq G(L/M_1)$,

(iii) Sind H_1 und H_2 zwei Untergruppen von $G(L/K)$ und $H_1 \leq H_2$, so gilt $L^{H_2} \subseteq L^{H_1}$,

(iv) Ist M ein Zwischenkörper der Körpererweiterung L/K und $\sigma \in G(L/K)$, so ist $G(L/\sigma(M)) = \sigma \circ G(L/M) \circ \sigma^{-1}$,

(v) Ist H eine Untergruppe von $G(L/K)$ und $\sigma \in G(L/K)$, so ist $\sigma(L^H) = L^{\sigma \circ H \circ \sigma^{-1}}$.

<u>Beweis</u>: (i) Die Körpererweiterung L/M ist normal nach Satz 217 und separabel nach Korollar 228.

(ii) $G(L/M_2) = \{\sigma \in \operatorname{Aut} L \mid \sigma(x) = x \ \forall x \in M_2\} \subseteq \{\sigma \in \operatorname{Aut} L \mid \sigma(x) = x \ \forall x \in M_1\} = G(L/M_1)$.

(iii) $L^{H_2} = \{a \in L \mid \sigma(a) = a \ \forall \sigma \in H_2\} \subseteq \{a \in L \mid \sigma(a) = a \ \forall \sigma \in H_1\} = L^{H_1}$.

(iv) $\tau \in G(L/\sigma(M)) \iff \tau \in \operatorname{Aut} L$ und $\tau(\sigma(a)) = \sigma(a) \ \forall a \in M$
$\iff \tau \in \operatorname{Aut} L$ und $(\sigma^{-1} \circ \tau \circ \sigma)(a) = a \ \forall a \in M \iff \sigma^{-1} \circ \tau \circ \sigma \in G(L/M)$
$\iff \tau \in \sigma \circ G(L/M) \circ \sigma^{-1}$.

(v) Für $a \in L$ gilt: $a \in L^H \Rightarrow \tau(a) = a \ \forall \tau \in H \Rightarrow (\sigma \circ \tau \circ \sigma^{-1})(\sigma(a)) = \sigma(\tau(a)) = \sigma(a) \ \forall \tau \in H$
$\Rightarrow \sigma(a) \in L^{\sigma \circ H \circ \sigma^{-1}}$. Damit ist $\sigma(L^H) \subseteq L^{\sigma \circ H \circ \sigma^{-1}}$ bewiesen.

Ebenfalls für $a \in L^H$ gilt $\sigma(a) \in L^{\sigma \circ H \circ \sigma^{-1}} \Rightarrow \sigma(\tau(a)) = (\sigma \circ \tau \circ \sigma^{-1})(\sigma(a)) = \sigma(a) \ \forall \tau \in H$
$\Rightarrow \tau(a) = a \ \forall \tau \in H \Rightarrow a \in L^H \Rightarrow \sigma(a) \in \sigma(L^H)$. Damit ist auch $L^{\sigma \circ H \circ \sigma^{-1}} \subseteq \sigma(L^H)$ bewiesen.

<u>Satz 235</u> (Hauptsatz der Galoistheorie) Es sei L/K eine endliche Galoiserweiterung. Es bezeichne $\mathcal{U}$ die Menge der Untergruppen der Galoisgruppe $G(L/K)$, d.h.

$$\mathcal{U} = \{H \mid H \leq G(L/K)\}$$

und $\mathcal{Z}$ die Menge der Zwischenkörper der Körpererweiterung L/K, d.h.

$$\mathcal{Z} = \{M \mid M \text{ ist Zwischenkörper der Körpererweiterung } L/K\}.$$

Dann gelten:

(i) Die Abbildungen $f: \mathcal{Z} \to \mathcal{U}$, $f(M) = G(L/M)$ und $g: \mathcal{U} \to \mathcal{Z}$, $g(H) = L^H$ sind bijektiv und zueinander invers (d.h. $L^{G(L/M)} = M \ \forall M \in \mathcal{Z}$ und $G(L/L^H) = H \ \forall H \in \mathcal{U}$) und kehren Mengeninklusionen um,

(ii) $[M:K] = [G(L/K) : f(M)] = [G(L/K) : G(L/M)] \quad \forall M \in \mathcal{Z}$,

(iii) $|H| = [L : g(H)] = [L : L^H] \quad \forall H \in \mathcal{U}$,

(iv) Für $M \in \mathcal{Z}$ ist M/K genau dann eine Galoiserweiterung wenn $f(M) \trianglelefteq G(L/K)$ (d.h. $G(L/M) \trianglelefteq G(L/K)$). Ist das der Fall, so ist die Abbildung $\varphi: G(L/K) \to G(M/K)$, die jedes $\sigma \in G(L/K)$ auf M einschränkt (d.h. $\varphi(\sigma): M \to M$, $\varphi(\sigma)(a) = \sigma(a) \ \forall a \in M$) ein Gruppenepimorphismus mit $\ker\varphi = G(L/M)$ und daher $G(M/K) \cong G(L/K)/G(L/M)$.

<u>Beweis</u>: (i) Ist $M \in \mathcal{Z}$, so ist L/M nach Lemma 234 (i) eine Galoiserweiterung und f daher wohldefiniert. Nach Satz 232 gilt

$$(g \circ f)(M) = g(G(L/M)) = L^{G(L/M)} = M = id_{\mathcal{Z}}(M) \qquad (\text{d.h. } g \circ f = id_{\mathcal{Z}}).$$

Ist $H \in \mathcal{U}$, so gilt

$$(f \circ g)(H) = f(L^H) = G(L/L^H) = H = id_{\mathcal{U}}(H) \qquad (\text{d.h. } f \circ g = id_{\mathcal{U}})$$

wegen Satz 233. D.h. f und g sind zueinander invers und daher bijektiv. Dass f und g Mengeninklusionen umkehren, wurde in Lemma 234 (ii) und (iii) bewiesen.

(ii) $$[G(L/K) : G(L/M)] \cdot [L:M] \overset{\text{Kor. 226}}{=} [G(L/K) : G(L/M)] \cdot |G(L/M)|$$

$$\overset{\text{Kor. 19 (i)}}{=} |G(L/K)| \overset{\text{Kor. 226}}{=} [L:K] \overset{\text{Satz 193 (ii)}}{=} [L:M] \cdot [M:K]$$

$$\Rightarrow [G(L/K) : G(L/M)] = [M:K].$$

(iii) Folgt sofort aus Satz 233 (ii).

(iv) Es sei $M \in \mathcal{Z}$ und M/K eine Galoiserweiterung. Dann $\exists! H \in \mathcal{U} : M = g(H) = L^H$ und $H = f(M) = G(L/M)$. Da M/K eine Galoiserweiterung ist, ist L^H/K normal und daher

$$g(H) = L^H = \sigma(L^H) \overset{\text{Lemma 234 (v)}}{=} L^{\sigma \circ H \circ \sigma^{-1}} = g(\sigma \circ H \circ \sigma^{-1}) \quad \forall \sigma \in G(L/K).$$

Da g bijektiv ist, folgt $H = \sigma \circ H \circ \sigma^{-1}$ $\forall \sigma \in G(L/K)$ und daher

$$G(L/M) = f(M) = H \trianglelefteq G(L/K).$$

Es sei nun umgekehrt $H \in \mathcal{U}$ und $H \trianglelefteq G(L/K)$. Dann $\exists! M \in \mathcal{Z} : H = f(M) = G(L/M)$ und $M = g(H) = L^H$. Da $G(L/M) \trianglelefteq G(L/K)$ gilt

$$f(\sigma(M)) = G(L/\sigma(M)) \overset{\text{Lemma 234 (iv)}}{=} \sigma \circ G(L/M) \circ \sigma^{-1} = G(L/M) = f(M) \quad \forall \sigma \in G(L/K).$$

Da f bijektiv ist, folgt $\sigma(M) = M$ $\forall \sigma \in G(L/K)$. Ist $\overline{K}$ ein algebraischer Abschluss von K mit $L \subseteq \overline{K}$ und $\psi : M \to \overline{K}$ ein Homomorphismus mit der Eigenschaft $\psi(x) = x$ $\forall x \in K$, so gibt es nach Satz 211 eine Fortsetzung $\tilde{\psi} : L \to \overline{K}$ von ψ. Da L/K eine normale Körpererweiterung ist, gilt $\tilde{\psi}(L) = L$, d.h. $\tilde{\psi}$ kann als Element von $G(L/K)$ aufgefasst werden und daher gilt $\psi(M) = \tilde{\psi}(M) = M$, d.h. die Körpererweiterung M/K ist normal. Da diese Körpererweiterung nach Korollar 228 auch separabel ist, ist M/K eine Galoiserweiterung.

Nach dem eben Bewiesenen ist $\sigma(M) = M$ $\forall \sigma \in G(L/K)$ wenn M/K eine Galoiserweiterung ist. Daher ist $\varphi(\sigma) \in G(M/K)$ $\forall \sigma \in G(L/K)$. Die Abbildung φ ist trivialerweise ein Gruppenhomomorphismus und surjektiv wegen Korollar 212: Es sei $\tau \in G(M/K)$ und $\overline{K}$ ein algebraischer Abschluss von K mit $L \subseteq \overline{K}$. Nach Korollar 212 gibt es einen Automorphismus $\psi : \overline{K} \to \overline{K}$, der τ fortsetzt. Da L/K eine normale Körpererweiterung ist, gilt $\psi(L) = L$. D.h. die Einschränkung σ von ψ auf L kann als Element von $G(L/K)$ aufgefasst werden und $\varphi(\sigma) = \tau$.

Schließlich gilt (für $\sigma \in G(L/K)$)

$$\sigma \in \ker\varphi \iff \varphi(\sigma) = \mathrm{id}_M \iff \sigma(a) = a \;\forall a \in M \iff \sigma \in G(L/M).$$

Aus Korollar 28 (Homomorphiesatz) folgt

$$G(L/K)/G(L/M) \cong G(M/K).$$

Beispiele: 1) $\mathbb{Q}(i)/\mathbb{Q}$ ist eine Galoiserweiterung mit Galoisgruppe $G(\mathbb{Q}(i)/\mathbb{Q}) = \{id_{\mathbb{Q}(i)}, \sigma\}$, wobei $\sigma : \mathbb{Q}(i) \to \mathbb{Q}(i)$ die komplexe Konjugation bezeichnet. (und $(G(\mathbb{Q}(i)/\mathbb{Q}), \circ)$ ist zu $(\mathbb{Z}_2, +)$ isomorph).

$$\begin{array}{ccc} \mathbb{Q}(i) = \mathbb{Q}(i)^{\{id_{\mathbb{Q}(i)}\}} & & \{id_{\mathbb{Q}(i)}\} = G(\mathbb{Q}(i)/\mathbb{Q}(i)) \\ | & & | \\ \mathbb{Q} = \mathbb{Q}(i)^{\{id_{\mathbb{Q}(i)}, \sigma\}} & & \{id_{\mathbb{Q}(i)}, \sigma\} = G(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}_2 \end{array}$$

2) $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ ist eine Galoiserweiterung ($\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ ist normal, da $\mathbb{Q}(\sqrt{2}, i)$ Zerfällungskörper von $(X^2-2)(X^2+1) \in \mathbb{Q}[X]$ ist und separabel, da char $\mathbb{Q} = 0$).
Es ist $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ und $1, \sqrt{2}$ ist eine Basis von $\mathbb{Q}(\sqrt{2})$ als $\mathbb{Q}$-Vektorraum. Weiters ist $m_{i, \mathbb{Q}(\sqrt{2})}(X) = X^2+1$, woraus folgt, dass $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] = 2$ und dass $1, i$ eine Basis von $\mathbb{Q}(\sqrt{2}, i)$ als $\mathbb{Q}(\sqrt{2})$-Vektorraum ist. Daher ist $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$ und $1, \sqrt{2}, i, \sqrt{2}i$ ist eine Basis von $\mathbb{Q}(\sqrt{2}, i)$ als $\mathbb{Q}$-Vektorraum.
Es ist $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id_{\mathbb{Q}(\sqrt{2})}, \varphi\}$, wobei $\varphi(x+y\sqrt{2}) = x - y\sqrt{2}$ (mit $x, y \in \mathbb{Q}$)
Für jede der beiden Abbildungen $id_{\mathbb{Q}(\sqrt{2})}$ und φ gibt es $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})]_s = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$ Fortsetzungen zu Automorphismen von $\mathbb{Q}(\sqrt{2}, i)$, die i auf $\pm i$ abbilden. Man erhält auf diese Weise, die folgenden vier Elemente von $G(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$:

$id_{\mathbb{Q}(\sqrt{2}, i)}$	$id_{\mathbb{Q}(\sqrt{2}, i)}(\sqrt{2}) = \sqrt{2}$, $id_{\mathbb{Q}(\sqrt{2}, i)}(i) = i$	$id_{\mathbb{Q}(\sqrt{2}, i)}(x+\sqrt{2}y+iu+i\sqrt{2}v) = x+\sqrt{2}y+iu+i\sqrt{2}v$
σ	$\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(i) = i$	$\sigma(x+\sqrt{2}y+iu+i\sqrt{2}v) = x-\sqrt{2}y+iu-i\sqrt{2}v$
τ	$\tau(\sqrt{2}) = \sqrt{2}$, $\tau(i) = -i$	$\tau(x+\sqrt{2}y+iu+i\sqrt{2}v) = x+\sqrt{2}y-iu-i\sqrt{2}v$
$\sigma \circ \tau = \tau \circ \sigma$	$(\sigma \circ \tau)(\sqrt{2}) = -\sqrt{2}$, $(\sigma \circ \tau)(i) = -i$	$(\sigma \circ \tau)(x+\sqrt{2}y+iu+i\sqrt{2}v) = x-\sqrt{2}y-iu+i\sqrt{2}v$

(jeweils mit $x, y, u, v \in \mathbb{Q}$)

Da $|G(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})| = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$, ist $G(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) = \{id_{\mathbb{Q}(\sqrt{2}, i)}, \sigma, \tau, \sigma \circ \tau\}$.
Da σ, τ und $\sigma \circ \tau$ Ordnung 2 haben, ist $(G(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}), \circ)$ zu $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ isomorph und $G(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ besitzt die folgenden fünf Untergruppen:
$\{id_{\mathbb{Q}(\sqrt{2}, i)}\}, \{id_{\mathbb{Q}(\sqrt{2}, i)}, \sigma\}, \{id_{\mathbb{Q}(\sqrt{2}, i)}, \tau\}, \{id_{\mathbb{Q}(\sqrt{2}, i)}, \sigma \circ \tau\}, \{id_{\mathbb{Q}(\sqrt{2}, i)}, \sigma, \tau, \sigma \circ \tau\}$.
Die Körpererweiterung $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ besitzt die drei (nichttrivialen) Zwischenkörper $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2}i)$.

Die Aussagen von Satz 235 können mit folgenden Diagrammen dargestellt werden:

$$\begin{tikzcd}[column sep=small]
 & \begin{matrix}\mathbb{Q}(\sqrt{2},i) \\ = \mathbb{Q}(\sqrt{2},i)^{\{id_{\mathbb{Q}(\sqrt{2},i)}\}}\end{matrix} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\begin{matrix}\mathbb{Q}(i) \\ = \mathbb{Q}(\sqrt{2},i)^{\{id_{\mathbb{Q}(\sqrt{2},i)},\sigma\}}\end{matrix} \arrow[dr, dash, "2"'] & \begin{matrix}\mathbb{Q}(\sqrt{2}) \\ = \mathbb{Q}(\sqrt{2},i)^{\{id_{\mathbb{Q}(\sqrt{2},i)},\tau\}}\end{matrix} \arrow[d, dash, "2"] & \begin{matrix}\mathbb{Q}(\sqrt{2}i) \\ = \mathbb{Q}(\sqrt{2},i)^{\{id_{\mathbb{Q}(\sqrt{2},i)},\sigma\circ\tau\}}\end{matrix} \arrow[dl, dash, "2"] \\
 & \begin{matrix}\mathbb{Q} \\ = \mathbb{Q}(\sqrt{2},i)^{\{id_{\mathbb{Q}(\sqrt{2},i)},\sigma,\tau,\sigma\circ\tau\}}\end{matrix} &
\end{tikzcd}$$

$\leftarrow$ Grad der Körpererweiterung $[\mathbb{Q}(\sqrt{2},i) : \mathbb{Q}(\sqrt{2},i)^H]$

$\leftarrow$ Grad der Körpererweiterung $[M:\mathbb{Q}]$

$$\begin{tikzcd}[column sep=small]
 & \begin{matrix}\{id_{\mathbb{Q}(\sqrt{2},i)}\} \\ = G(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}(\sqrt{2},i))\end{matrix} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\begin{matrix}\{id_{\mathbb{Q}(\sqrt{2},i)},\sigma\} \\ = G(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}(i))\end{matrix} \arrow[dr, dash, "2"'] & \begin{matrix}\{id_{\mathbb{Q}(\sqrt{2},i)},\tau\} \\ = G(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}(\sqrt{2}))\end{matrix} \arrow[d, dash, "2"] & \begin{matrix}\{id_{\mathbb{Q}(\sqrt{2},i)},\sigma\circ\tau\} \\ = G(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}(\sqrt{2}i))\end{matrix} \arrow[dl, dash, "2"] \\
 & \begin{matrix}\{id_{\mathbb{Q}(\sqrt{2},i)},\sigma,\tau,\sigma\circ\tau\} \\ = G(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})\end{matrix} &
\end{tikzcd}$$

$\leftarrow$ Ordnung $|H|$

$\leftarrow$ Index $[G(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}) : G(\mathbb{Q}(\sqrt{2},i)/M]$

Da $G(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$ abelsch ist, sind alle Untergruppen H von $G(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$ Normalteiler von $G(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q})$ und für alle Zwischenkörper M der Körpererweiterung $\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}$ ist $M/\mathbb{Q}$ eine Galoiserweiterung.
Nach Satz 235 besitzt die Körpererweiterung $\mathbb{Q}(\sqrt{2},i)$ außer $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2}i)$ keine weiteren (echten) Zwischenkörper.