§1. Galois-Theorie

Galoistheorie vergleicht Körpererweiterungen mit endlichen Gruppen.
Die Grundsätze sind Galoiserweiterungen und Galoisgruppen:

1.1 Definition: Sei L/K eine endliche Körpererweiterung. L/K heißt Galoiserweiterung (oder galoissche Erweiterung), wenn L/K normal und separabel ist. (Évariste Galois, 1811–1832) kurze Biografie z.B. auf mathshistory.st-andrews.ac.uk

Die Gruppe $\mathrm{Aut}_K(L) =$

$$\{\varphi: L \to L \text{ Körperautomorphismus mit } \varphi|_K = \mathrm{id}_K\}$$

heißt dann Galoisgruppe von L/K.
Bezeichnung: $\mathrm{Gal}(L/K)$ oder $G(L/K)$

Also: $|\mathrm{Gal}(L/K)| = [L:K] = [L:K]_s = |\{\varphi: L \to \bar{K}\ K\text{-Homom.}\}| < \infty$
Das Thema der Galoistheorie ist die Interaktion zwischen der Gruppentheorie von $\mathrm{Gal}(L/K)$ und der Körpertheorie von L/K.

Ausführliches Beispiel:
Sei $K = \mathbb{Q}$, $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ und L der Zerfällungskörper von $f(x)$
L ist also der kleinste Teilkörper von $\mathbb{C}$, der $\mathbb{Q}$ enthält sowie drei Nullstellen von f: $\sqrt[3]{2} \in \mathbb{R}$, $\sqrt[3]{2} \cdot e^{2\pi i/3}$ und $\sqrt[3]{2} \cdot e^{4\pi i/3}$
L enthält $\mathbb{Q}(\sqrt[3]{2})$, d.h. $L \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$, wir bestimmen $[\subseteq L: \mathbb{Q}]$ als Produkt $[L: \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}): \mathbb{Q}]$ (Gradformel)
Satz von Kronecker $\Rightarrow [\mathbb{Q}(\sqrt[3]{2}): \mathbb{Q}] = \deg f = 3$
Behauptung: $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) = (\mathbb{Q}(\sqrt[3]{2}))(e^{2\pi i/3})$
Beweis der Behauptung: $L \ni \sqrt[3]{2}, \sqrt[3]{2} \cdot e^{2\pi i/3} \Rightarrow L \ni e^{2\pi i/3} \Rightarrow L \supset \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$
$\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) \ni e^{4\pi i/3}, \sqrt[3]{2} e^{2\pi i/3}, \sqrt[3]{2} \cdot e^{4\pi i/3} \Rightarrow \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}) \supset L$
Also ist $[\mathbb{Q}(\sqrt[3]{2})(e^{2\pi i/3}): \mathbb{Q}(\sqrt[3]{2})]$ zu bestimmen.
$e^{2\pi i/3}$ erfüllt $x^3 - 1 = 0$. Nullstellen von $x^3 - 1$ sind $1, e^{2\pi i/3}, e^{4\pi i/3}$
$x^3 - 1 = (x-1)(x^2+x+1) \Rightarrow x^2+x+1$ hat Nullstellen $e^{2\pi i/3}, e^{4\pi i/3}$
x^2+x+1 ist irreduzibel über $\mathbb{Q}$ und über $\mathbb{Q}(\sqrt[3]{2})$ warum?

$\Rightarrow x^2+x+1$ ist das Minimalpolynom von $e^{2\pi i/3}$ über $\mathbb{Q}$ und über $\mathbb{Q}(\sqrt[3]{2})$

$\Rightarrow [L:\mathbb{Q}(\sqrt[3]{2})]=2 \Rightarrow [L:\mathbb{Q}]=2\cdot 3=6$

Jetzt bestimmen wir die $\mathbb{Q}$-Automorphismen von L:

$L/\mathbb{Q}$ separabel $\Rightarrow |\mathrm{Aut}_{\mathbb{Q}=\mathbb{Q}}(L)| = [L:\mathbb{Q}]=6$, es gibt also 6 $\mathbb{Q}$-Autom $\sigma: L\to L$, einer davon ist $id: L\to L$

Sei $\sigma: L\to L$ ein $\mathbb{Q}$-Automorphismus von L. $\sigma|_{\mathbb{Q}}=id$, also liegt σ fest, wenn die Bilder von $\sqrt[3]{2}$, $\sqrt[3]{2}\,e^{2\pi i/3}$ und $\sqrt[3]{2}\,e^{4\pi i/3}$ festliegen, genaue Begründung?

da $\sigma^*(x^3-2)=x^3-2$ und L der Zerfällungskörper ist.

(Auch $\sigma^*(x^2+x+1)=x^2+x+1$, also muß $\sigma(e^{2\pi i/3})$ entweder $e^{2\pi i/3}$ oder $e^{4\pi i/3}$ sein.)

σ injektiv $\Rightarrow$ σ permutiert die drei Nullstellen von x^3-2 und ist dadurch festgelegt $\Rightarrow$ die Abbildung

$$\begin{array}{ccc} \mathrm{Aut}_{\mathbb{Q}}(L) & \longrightarrow & \mathrm{Sym}\left(\left\{\sqrt[3]{2},\ \sqrt[3]{2}\,e^{2\pi i/3},\ \sqrt[3]{2}\,e^{4\pi i/3}\right\}\right) \simeq \Sigma_3 \\ \Psi & & \text{(Symm Gruppe)} \\ \sigma & \longmapsto & \sigma|_{\left\{\sqrt[3]{2},\ \sqrt[3]{2}e^{2\pi i/3},\ \sqrt[3]{2}e^{4\pi i/3}\right\}} \end{array}$$

ist injektiv.

Da $|\mathrm{Aut}_{\mathbb{Q}}(L)|=6=3!=|\Sigma_3|$, muß diese Abbildung sogar bijektiv sein.

Wie sehen die 6 Elemente von $\mathrm{Aut}_{\mathbb{Q}}(L)$ genau aus?

Wähle eine Permutation: $\sigma: \sqrt[3]{2}\mapsto\sqrt[3]{2}$

$\sqrt[3]{2}\cdot e^{2\pi i/3}\mapsto \sqrt[3]{2}\,e^{4\pi i/3}$, also: $\sqrt[3]{2}\,e^{4\pi i/3}\mapsto \sqrt[3]{2}\,e^{2\pi i/3}$

σ ist die Einschränkung der komplexen Konjugation auf L warum?

Beobachtung: $\sigma|_{\mathbb{Q}(\sqrt[3]{2})}=id|_{\mathbb{Q}(\sqrt[3]{2})}$, die reellen Zahlen sind die Fixpunkte der komplexen Konjugation. Also besteht $\mathbb{Q}(\sqrt[3]{2})\subset\mathbb{R}$ aus Fixpunkten.

Gibt es noch weitere Fixpunkte in L oder ist $L\cap\mathbb{R}=\mathbb{Q}(\sqrt[3]{2})$?

Behauptung: $L\cap\mathbb{R}=\mathbb{Q}(\sqrt[3]{2})$, d.h. $\mathbb{Q}(\sqrt[3]{2})=\{a\in L: a=\bar{a}\}$, genau die σ-Fixpunkte

Beweis der Behauptung: Wir bestimmen eine $\mathbb{Q}$-Basis von L und wenden σ auf $\mathbb{Q}$-Linearkombinationen der Basiselemente an:

$\mathbb{Q}(\sqrt[3]{2})$ hat $1, \sqrt[3]{2}, \sqrt[3]{4}$ als $\mathbb{Q}$-Basis warum?

eine Basis von L über $\mathbb{Q}(\sqrt[3]{2})$ ist $1, e^{2\pi i/3}$ warum? $\Rightarrow$

eine $\mathbb{Q}$-Basis von L ist: $1, \sqrt[3]{2}, \sqrt[3]{4}, e^{2\pi i/3}, e^{2\pi i/3}\cdot\sqrt[3]{2}, e^{2\pi i/3}\cdot\sqrt[3]{4}$

σ anwenden $\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$ $\downarrow$

$1, \sqrt[3]{2}, \sqrt[3]{4}, e^{4\pi i/3}, e^{4\pi i/3}\cdot\sqrt[3]{2}, e^{4\pi i/3}\cdot\sqrt[3]{4}$ Begründung?

Wie schreibt man $e^{4\pi i/3}$ in der gewählten $\mathbb{Q}$-Basis?

$e^{2\pi i/3}$ und $e^{4\pi i/3}$ sind Nullstellen von x^2+x+1, $e^{4\pi i/3} = (e^{2\pi i/3})^2$

$\Rightarrow e^{4\pi i/3} = -1 - e^{2\pi i/3}$, also: $\sigma: e^{2\pi i/3} \mapsto -1 - e^{2\pi i/3}$

$\Rightarrow a\cdot 1 + b\sqrt[3]{2} + c\sqrt[3]{4} + d e^{2\pi i/3} + f e^{2\pi i/3}\sqrt[3]{2} + g e^{2\pi i/3}\cdot\sqrt[3]{4}$ $(a,b,c,d,f,g \in \mathbb{Q})$

$\downarrow \sigma$

$a\cdot 1 + b\sqrt[3]{2} + c\sqrt[3]{4} - d - d e^{2\pi i/3} - f\sqrt[3]{2} - f e^{2\pi i/3}\sqrt[3]{2} - g\sqrt[3]{4} - g e^{2\pi i/3}\sqrt[3]{4}$

Koeffizientenvergleich $\Rightarrow$ das ist ein σ-Fixpunkt genau dann, wenn $d=f=g=0$ (und a,b,c beliebig in $\mathbb{Q}$) $\Rightarrow$ Behauptung

σ ist ein Element von $Gal(L/K)$, es hat Ordnung 2 und erzeugt die Untergruppe $U = \{id, \sigma\} \cong \mathbb{Z}/2\mathbb{Z} \cong \Sigma_2$ was wird permutiert?

$\Rightarrow \mathbb{Q}(\sqrt[3]{2}) = \{a \in L : a = \tau(a)\ \forall \tau \in U\}$, die Fixpunkte der Untergruppe U

Interpretation: Wenn L und $\mathbb{Q}$ gegeben sind und $Gal(L/\mathbb{Q})$, dann können wir den Zwischenkörper $\mathbb{Q}(\sqrt[3]{2})$ als Fixkörper der Untergruppe $U < Gal(L/\mathbb{Q})$ finden.

Also: Untergruppe $\rightsquigarrow$ Zwischenkörper.

Diese Zuordnung funktioniert allgemein – das ist eine Grundidee der Galoistheorie.

1.2 Definition: Sei L ein Körper und $U \subset Aut(L)$ eine Untergruppe der der Automorphismengruppe von L. Dann ist die Menge $L^U := \{a \in L : \sigma(a) = a\ \forall \sigma \in U\}$ ein Körper und heißt der Fixkörper von U.

Beweis, daß L^U ein Körper ist: $\sigma(0)=0, \sigma(1)=1\ \forall\sigma \Rightarrow 0,1 \in L^U$

$\sigma(a+b) = \sigma(a)+\sigma(b), \sigma(a\cdot b) = \sigma(a)\cdot\sigma(b) \Rightarrow a+b, a\cdot b \in L^U$ für $a,b \in L^U$

$\sigma(a^{-1})\sigma(a) = \sigma(1) = 1 \Rightarrow \sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1}$ für $a \in L^U - \{0\}$

Beispiel: wähle $U = \{id\} < Aut(L) \Rightarrow L^U = L$

Interessanteres Beispiel: $U = Gal(L/K)$ für Galoiserweiterung

1.3 Proposition: Sei L/K eine Galoiserweiterung mit Galoisgruppe $G = Gal(L/K)$. Dann ist $L^G = K$, d.h. der Grundkörper K ist der Fixkörper der Galoisgruppe.

(Je größer die Untergruppe G, desto mehr Bedingungen muß ein Fixpunkt erfüllen. Deshalb ist $L^G = K$ kleinstmöglich.)

Beweis: Alle $\sigma \in G$ sind K-Automorphismen $\Rightarrow K \subset L^G$.

Umgekehrt ist $L^G \subset K$ zu zeigen. Sei $a \in L - K$, zz $a \notin L^G$, d.h. zz $\exists \tilde{\sigma} \in G : \tilde{\sigma}(a) \neq a$

$a \notin K$, aber $a \in L \Rightarrow K \subsetneq K(a) \subset L$, $2 \leq [K(a):K] = \deg m_{a,K}$

L/K separabel $\Rightarrow$ alle Elemente von L sind separabel über K, auch a

$\Rightarrow m_{a,K}$ hat nur einfache Nullstellen, aber Grad $\geq 2 \Rightarrow$ es gibt mindestens eine weitere Nullstelle $b \neq a$. L normal $\Rightarrow b \in L \subset \bar{K}$

Satz von Kronecker (oder Algebra, Proposition 6.3): $K(a) \xrightarrow{\sigma} K(b)$ durch einen K-Isomorphismus. Diesen K-Isomorphismus interpretieren wir als

Details?

K-Homomorphismus $\sigma : K(a) \to \bar{K}$ mit Bild $\sigma(K(a)) = K(b)$.

Da $\bar{K}$ algebraisch abgeschlossen ist, existiert eine Erweiterung

$$\begin{array}{ccc} K(a) & \xrightarrow{\sigma} & \bar{K} \\ \cap & \nearrow_{\tilde{\sigma}} & \\ L & & \end{array} \qquad \tilde{\sigma} : L \to \bar{K} \text{ mit } \tilde{\sigma}|_{K(a)} = \sigma$$

(Algebra, Theorem 6.4)

wie wird 6.4 genau angewandt?

L normal $\Rightarrow \tilde{\sigma}$ hat Bild L, d.h. $\tilde{\sigma}$ ist in $\mathrm{Aut}_K(L) = G$.

Und $\tilde{\sigma}(a) = \sigma(a) = b$ nach Konstruktion. $\square$

Die Voraussetzung L/K Galois wird im Beweis verwendet, ist aber auch wirklich nötig: $L = \mathbb{Q}(\sqrt[3]{2})$ hat $\mathrm{Aut}_{\mathbb{Q}}(L) = \mathrm{id}$, $L^{\mathrm{Aut}_{\mathbb{Q}}(L)} = L \neq K = \mathbb{Q}$.

Durch die beiden Untergruppen G und $\{\mathrm{id}\}$ erhält man die Fixkörper $L^G = K$ und $L^{\{\mathrm{id}\}} = L$. Durch andere Untergruppen vielleicht weitere Fixkörper zwischen K und L? Kann man neue Galoiserweiterungen herstellen von der Form L/L^H für H eine Gruppe von Automorphismen?

1.4 Proposition: Sei L ein Körper und $H \subset \mathrm{Aut}(L)$ eine endliche Untergruppe. Dann ist L/L^H eine Galoiserweiterung mit Galoisgruppe $\mathrm{Gal}(L/L^H) = H$ und es gilt $[L:L^H] = |H|$.

Daraus folgt, daß jede endliche Gruppe als Galoisgruppe vorkommt (siehe Übungen).
An L werden keine Voraussetzungen gestellt.

Beweis von 1.4.
$L^H = \{a \in L : \sigma(a) = a \ \forall \sigma \in H\}$
Behauptung 1: L/L^H ist normal, separabel und algebraisch
Normal bedeutet: L ist Zerfällungskörper einer Menge von Polynomen in $L^H[x]$. Falls dasstimmt, hat $a \in L$ ein Minimalpolynom $m_{a,L^H} \in L^H[x]$, also mit Koeffizienten in L^H. Automorphismen $\sigma \in H$ lassen die Koeffizienten von m_{a,L^H} fest, permutieren also die Nullstellen von m_{a,L^H}. Mit a ist also auch jedes $\sigma(a)$ ($\sigma \in H$) eine Nullstelle von m_{a,L^H}, und es könnte noch weitere Nullstellen geben.
Sei $\{\sigma(a) : \sigma \in H\} = \{a = a_1, a_2, \dots, a_n\}$ (da H endlich). Unser Kandidat für $m_{a,L^H}(x)$ ist $f_a(x) := \prod_{i=1}^{n} (x - a_i) \in L[x]$. Für Behauptung 1 brauchen wir nur, daß $f_a(x) \in L^H[x]$, am Ende des Beweises von 1.4 wird $f_a = m_{a,L^H}$ folgen.
Sei $\sigma \in H$, zz die Koeffizienten von f_a sind fix unter σ, d.h. $\sigma^*(f_a) = f_a$.
$\sigma^*(x - a_i) = x - \sigma(a_i) = x - a_j$ für ein j, denn σ permutiert die a_i mit inverser Permutation $\sigma^{-1} \in H \Rightarrow \sigma^* f_a = f_a \Rightarrow f_a(x) \in L^H[x]$
$f_a(a) = 0 \Rightarrow a$ ist Nullstelle eines Polynoms in $L^H[x]$.
Alle anderen Nullstellen von f_a liegen auch in L.
$\Rightarrow L/L^H$ ist Zerfällungskörper von $\mathcal{A} = \{f_a : a \in L\} \subset L^H[x]$
$\Rightarrow L/L^H$ ist normal
Jedes $a \in L$ ist Nullstelle eines Polynoms in $L^H[x]$ – z.B. $f_a(x)$ – also ist L/L^H algebraisch (später sehen wir: L/L^H ist endlich, daraus folgt algebraisch warum?).
Noch zz L/L^H ist separabel: Für $a \in L$ hat f_a nach Konstruktion nur einfache Nullstellen. $m_{a,L^H}(x) \mid f(x)$ warum? $\Rightarrow m_{a,L^H}(x)$ hat auch nur einfache Nullstellen $\Rightarrow a$ ist separabel $\Rightarrow L/L^H$ ist separabel
Folgt hieraus schon $m_{a,L^H} = f_a$?

Ist damit schon gezeigt, daß $L|L^H$ eine Galoiserweiterung ist?

Behauptung 2: $[L:L^H] \leq |H|$

Angenommen $|H| \lneq [L:L^H]$. Dann ist ein Widerspruch gesucht.
Wenn $[L:L^H] < \infty$, dann $\exists S \subset L$, S endliche Menge mit $L = L^H(S)$,
also $[L^H(S):L^H] > |H|$
Wenn $[L:L^H] \neq \infty$ gibt es auch so ein S (endlich): Denn L ist
algebraisch über L^H, $L = L^H(\tilde{S})$ für eine Menge $\tilde{S} \subset L$, aus der
man induktiv Elemente wählen kann mit
$L^H \subset L^H(s_1) \subset L^H(s_1,s_2) \subset \dots \subset L^H(s_1, s_2, \dots, s_n) \subset \dots$
Wenn man nach endlich vielen Schritten L erreicht, z.B. $L = L^H(s_1, \dots, s_n)$,
hat man $S = \{s_1, \dots, s_n\}$ gefunden. Wenn das nicht geht, sind die
Inklusionen echt und für großes n ist $[L^H(s_1, \dots, s_n):L^H] \geq |H|$.
Also können wir so ein endliches $S \subset L$ wählen mit

$$[L^H(S):L^H] > |H|.$$

Sei $M := L^H(S)$, d.h. $L^H \subset M \subset L$ ist eine Kette von Körpererweiterungen.
$M|L^H$ ist nach Konstruktion endlich, vom Grad $[M:L^H] \geq |H|$.
Wir zeigen, daß es so ein M nicht geben kann, und erhalten damit
den gewünschten Widerspruch.
$M|L^H$ ist eine separable Erweiterung: Denn $M \subset L$, also ist
$a \in M$ Nullstelle von $f_a(x) \in L^H[x]$, wie oben konstruiert. Daraus
folgt, daß alle $a \in M$ separabel sind. warum?
Weil $M|L^H$ separabel ist, dürfen wir den Satz vom primitiven Element
(Algebra, Theorem 6.13) anwenden nachschauen und Voraussetzungen prüfen
$\Rightarrow \exists c \in M$ mit $M = L^H(c)$, d.h. M ist
eine einfache Erweiterung von L^H
Das Element $c \in M \subset L$ ist Nullstelle von f_c, sein Minimalpolynom
$m_{c,L^H}(x)$ teilt also $f_c(x)$. Daraus folgt:

$[M:L^H] = [L^H(c):L^H] = \deg(m_{c,L^H}) \leq \deg(f_c) \leq |H|$

Also: $[M:L^H] \leq |H| \lneq [M:L^H]$ ↯

das ist der gesuchte Widerspruch

Begründung für jede (Un)Gleichung?

Die Annahme war also falsch und Behauptung 2 ist gezeigt:

$$[L:L^H] \leq |H|$$

Also ist L/L^H endlich, wegen Behauptung 1 also eine Galoiserweiterung.

Behauptung 3: $[L:L^H] = |H|$, $H = Gal(L/L^H)$ und für $a \in L$ ist

$$f_a(x) = m_{a,L^H}(x) = \prod_{\sigma \in Gal(L/L^H)} (x - \sigma(a))$$

L^H ist der Fix Körper von H, also gilt $\forall a \in L^H \; \forall \sigma \in H: a = \sigma(a)$

$\Rightarrow H \subset Aut_{L^H}(L)$, d.h. die Elemente von H sind L^H-Homomorphismen

L/L^H Galoiserweiterung bedeutet $Gal(L/L^H) = Aut_{L^H}(L)$

$\Rightarrow |H| \leq |Aut_{L^H}(L)| = [L:L^H] \leq |H| \Rightarrow |H| = [L:L^H]$ (Beh. 2)

$\Rightarrow H = Aut_{L^H}(L) = Gal(L/L^H)$

Für $a \in L$ folgt auch: $f_a(x) = \prod_{\sigma \in Gal(L/L^H)} (x - \sigma(a))$. Wegen $m_{a,L^H}(x) \mid f_a(x)$ und $\sigma(a)$ Nullstelle von $m_{a,L^H}(x)$ $\forall \sigma \in Gal(L/L^H)$ folgt $f_a = m_{a,L^H}$. □

Die Beweise von 1.3 und 1.4 sind sehr komplex und harte Arbeit. Damit ist aber schon der schwierigste Schritt zum Hauptergebnis gemacht.

Der nun folgende Hauptsatz der Galoistheorie stellt eine präzise Beziehung her zwischen endlichen Körpererweiterungen und ihren Zwischenkörpern einerseits und endlichen Gruppen und ihren Untergruppen andererseits.

1.5 Theorem (Hauptsatz der Galoistheorie): Sei $L|K$ eine Galois-Erweiterung, $\mathcal{U} := \{H : H < Gal(L|K)$ Untergruppe$\}$ die Menge aller Untergruppen von $Gal(L|K)$ und $\mathcal{Z} := \{M : K < M < L\}$ die Menge der Zwischenkörper.

Dann ist $L|M$ eine Galoiserweiterung $\forall M \in \mathcal{Z}$.

Die Abbildungen $\alpha : \mathcal{Z} \longrightarrow \mathcal{U},\ M \mapsto Gal(L|M)$

und $\beta : \mathcal{U} \longrightarrow \mathcal{Z},\ H \mapsto L^H$

sind zueinander inverse Bijektionen.

α und β kehren Inklusionen um: $M_1 \subset M_2 \Rightarrow \alpha(M_1) \supset \alpha(M_2)$

$H_1 \subset H_2 \Rightarrow \beta(H_1) \supset \beta(H_2)$

Für $\sigma \in Gal(L|K)$ und $H \in \mathcal{U}$ gilt: $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$.

Eine normale Körpererweiterung $M = \beta(U)$ entspricht einer normalen Untergruppe $H = \alpha(M)$, das heißt:

$M|K$ normal $\Leftrightarrow Gal(L|M) \trianglelefteq Gal(L|K)$

In diesem Fall gibt es einen surjektiven Gruppenhomomorphismus

$$\varphi : Gal(L|K) \longrightarrow Gal(M|K)$$

mit $\ker(\varphi) = Gal(L|M)$ und es gilt die "Kürzungsregel"

$$Gal(M|K) \simeq Gal(L|K) / Gal(L|M).$$

Daraus folgt z.B.: $L|K$ Galois $\Rightarrow$ es gibt nur endlich viele Zwischenkörper $K < L < M$.

$M|K$ ist im Allgemeinen keine Galoiserweiterung. Gegenbeispiel?

Galoistheorie gibt es auch für unendliche Erweiterungen, in der algebraischen Zahlentheorie, für Differentialgleichungen, ...

Vor dem Beweis (die Hauptarbeit wurde in 1.3 und 1.4 schon geleistet) folgt nun ein ausführliches Beispiel, in dem die Galois-Korrespondenz sichtbar wird.