Der Hauptsatz der Galoistheorie[†]

Zunächst einige Vorüberlegungen.

Transitive G-Mengen

Es sei G eine Gruppe und M eine Menge, auf welcher G transitiv operiert. Dann gilt für eines (und damit für jedes) $m \in M$, daß die Abbildung $b : G \to M,\ g \mapsto g \cdot m$ surjektiv ist. Mit anderen Worten: wir haben die Identität $G \cdot m = M$. Es bezeichen G_m den Stabilisator von m, d.h. die Menge der $g \in G$ mit $g \cdot m = m$. Dann ist G_m eine Untergruppe von G und die Abbildung $b : G \to M$ faktorisiert eindeutig über die G-Menge G/G_m. Genauer haben wir ein kommutatives Diagramm von G-Mengen:

$$\begin{array}{ccc} G & \xrightarrow{b} & M \\ {\scriptstyle\pi}\downarrow & & \| \\ G/G_m & \xrightarrow{\bar{b}} & G \cdot m \end{array}$$

wobei $\pi : G \to G/G_m$ die kanonische Projektion $g \mapsto g \cdot G_m$ bezeichnet. Die Abbildung $\bar{b}$ ist sogar bijektiv, insbesondere ein *Isomorphismus* in der Kategorie $\mathcal{T}$ der (transitiven) G-Mengen. *Jede* transitive G-Menge ist also von der Form G/H mit einer geeigneten Untergruppe H.
Es sei nun $f : M \to M'$ ein Morphismus transitiver G-Mengen. Dann ist f ein Epimorphismus, denn für beliebiges $m \in M$ gilt

$$M' = G \cdot f(m) = f(G \cdot m) = f(M).$$

Desweiteren ist f bereits durch das Bild $f(m) \in M'$ von m eindeutig bestimmt, denn $f(g \cdot m) = g \cdot f(m)$ und $G \cdot m = M$. Umgekehrt kann $f(m) \in M'$ ganz beliebig ausfallen.

Galoistheorie

Es sei nun L/K eine endliche galoissche Körpererweiterung mit Galoisgruppe G. Es bezeichne $\mathcal{K}$ die opposite Kategorie der Kategorie der Zwischenkörper (Morphismen in letzterer sind Körpermorphismen, welche auf K die Identität induzieren). Mit anderen Worten: $\mathrm{Mor}_{\mathcal{K}}(Z, Z') = \mathrm{Hom}_K(Z', Z)$. Es bezeichen $\mathcal{U}$ die Menge der Untergruppen von G. Der Hauptsatz der Galoistheorie läßt sich lesen als:

(i) Die Abbildung $\mathrm{Ob}\,\mathcal{K} \to \mathcal{U}$,

$$Z \mapsto G_Z := \{g \in G \mid g|_Z = \mathrm{id}_Z\}$$

ist bijektiv mit der Inversen

$$H \mapsto L^H := \{\alpha \in L \mid \forall g \in G : g\alpha = \alpha\}.$$

(ii) Für jedes $Z \in \mathrm{Ob}\,\mathcal{K}$ haben wir eine kanonischen Isomorphismus

$$G/G_Z \cong \mathrm{Hom}_K(Z, L)$$

$$g \cdot G_Z \mapsto g \circ i_Z$$

von G-Mengen, wobei $i_Z : Z \to L, z \mapsto z$ die kanonische Inklusion bezeichnet.

Dabei ist $\mathrm{Hom}_K(Z, L)$ eine G-Menge vermöge der Verknüpfung $(g, h) \mapsto g \circ h$.

[†]oder eine Lösung zur Aufgabe 3 des Übungsblattes 3.

Kategoriell

Wir betrachten nun den Funktor $E : \mathcal{K} \to \mathcal{T}$ der Zwischenkörper in die Kategorie der transitiven G-Mengen, welcher gegeben ist durch

$$Z \mapsto \mathrm{Hom}_K(Z, L) =: E(Z).$$

Auf Morphismen ist dieser wie folgt erkärt. Sei $f \in \mathrm{Mor}_{\mathcal{K}}(Z, Z') = \mathrm{Hom}_K(Z', Z)$. Dann induziert f eine kanonische Abbildung

$$E(f) := f^* : \mathrm{Hom}_K(Z, L) \to \mathrm{Hom}_K(Z', L),$$

gegeben durch die Zuordnung

$$i \mapsto i \circ f.$$

Dadurch wird E tatsächtlich zu einem kovarianten Funktor, denn f^* verträgt sich mit den beiden G-Mengenstrukturen.
Wir behaupten, daß E volltreu ist. Zunächst ist E *treu*, denn obiges i ist stets injektiv (als Abbildung) und f damit durch $E(f)$ bereits eindeutig bestimmt. Andererseits ist E *voll*, denn ist

$$\nu : \mathrm{Hom}_K(Z, L) \to \mathrm{Hom}_K(Z', L)$$

ein Morphismus von G-Mengen, so ist ν bereits durch $\nu(i_Z)$ eindeutig bestimmt, denn wir haben es mit *transitiven* G-Mengen zu tun (s.o.). Wir behaupten, daß $\nu(i_Z)(Z') \subseteq Z$. Hierzu greifen wir auf (i) aus der Galoistheorie zurück: für jedes $g \in G_Z$ gilt

$$g \circ \nu(i_Z) = \nu(g \circ i_Z) = \nu(i_Z),$$

mithin induziert g auf $\nu(i_Z)(Z')$ die Identität, weswegen dieser Körper in Z enthalten sein muß. Also faktorisiert ν über i_Z, d.h. wir haben ein kommutatives Diagramm (in der oppositen Kategorie $\mathcal{K}^0$):

$$\begin{array}{ccc} Z & \xrightarrow{\nu(i_Z)} & L \\ \| & & \uparrow{\scriptstyle i_Z} \\ Z & \xrightarrow{f} & Z' \end{array}$$

mit einem $f \in \mathrm{Hom}_K(Z, Z')$. Damit gilt

$$E(f)(i_Z) = f^*(i_Z) = i_Z \circ f = \nu(i_Z)$$

und da es sich um transitive G-Mengen handelt, folgt hieraus bereits $E(f) = \nu$. Daher ist E voll.
Aus dem Abschnitt über transitive G-Mengen wissen wir bereits, daß jede transitive G-Menge isomorph ist zu einer G-Menge der Form G/H, H eine Untergruppe von G. Der Hauptsatz der Galoistheorie (i)+(ii) sagt uns, daß alle diese G-Mengen im Bild von E liegen, weswegen Proposition 1.2.8 aus der Vorlesung zeigt, daß E tatsächlich eine Äquivalenz von Kategorien ist. Das zeigt (a). (b) und (c) ergeben sich via $X := L$ ebenfalls aus obiger Diskussion.
Um (d) einzusehen, betrachten wir folgende Situation. Es sei ν analog zur obigen Situation ein beliebiger Morpismus $E(Z) \to E(Z) = \mathrm{Hom}_K(Z, L)$ in $\mathcal{T}$. Punkt (ii) der Galoistheorie sagt uns, daß es zu einem beliebigen (aber festen) $i \in \mathrm{Hom}_K(Z, L)$ ein

$g \in G$ gibt mit $\nu(i) = g \circ i$. Wegen $G = \mathrm{Hom}_K(L, L) = E(L)$ haben wir also folgendes kommutatives Diagramm von (transitiven) G-Mengen

$$\begin{array}{ccc} E(L) & \xrightarrow{h \mapsto g \circ h} & E(L) \\ {\scriptstyle h \mapsto h \circ i}\downarrow & & \downarrow{\scriptstyle h \mapsto h \circ i} \\ E(Z) & \xrightarrow{\nu} & E(Z) \end{array}$$

Es sei angemerkt, daß per Definitionem $E(i) = i^* : h \mapsto h \circ i$ gilt. Jedes ν entspringt in diesem Sinne aus einem $g \in G$. Umgekehrt gibt jedes $g \in G$ zu einem $\nu = g \circ i_Z$ Anlaß. Das zeigt, daß sich die natürlichen Transformationen $E \to E$ mit G identifizieren lassen und es sich insbesondere um natürliche Isomorphismen handelt.

Betrachten wir die Komposition $F : \mathcal{K} \to \underline{Men}$ von E mit dem Vergißfunktor, so ist klar, daß die eben betrachteten natürlichen Transformationen von E auch ebensolche von F sind. Daß es nicht *weitere* natürliche Transformationen $\eta : F \to F$ gibt, ergibt sich unmittelbar aus dem folgenden kommutativen Diagramm, denn es zeigt (in Analogie zur Aufgabe 2 (b)), daß η stets aus Abbildungen besteht, welche die G-Mengenstruktur respektieren:

$$\begin{array}{ccc} F(L) & \xrightarrow{F(g)} & F(L) \\ {\scriptstyle \eta_L}\downarrow & & \downarrow{\scriptstyle \eta_L} \\ F(L) & \xrightarrow{F(g)} & F(L) \end{array}$$

Dabei ist $g \in G$ beliebig und „wieder“ gilt $F(g) : h \mapsto h \circ g$. Daher respektiert η_L die G-Mengenstruktur auf $E(L)$ und jedes η_Z für $Z \in \mathrm{Ob}\,\mathcal{K}$ respektiert die entsprechende auf $E(Z)$ ebenfalls, denn die G-Mengenstruktur auf $E(Z)$ ist gerade das Bild der G-Mengenstruktur von $E(L)$ unter dem G-Mengenmorphismus $E(i_Z) : E(L) \to E(Z)$ und η_Z ist durch η_L bereits eindeutig bestimmt (in der Kategorie der transitiven G-Mengen sind alle Morphismen epimorph).