§6.9 ~~§ 11~~ Explizite Bestimmung von Galoisgruppen

Literatur: van der Waerden, Algebra I, §66.

Die allgemeine Theorie sagt uns leider noch nicht, wie man explizit Galoisgruppen bestimmen kann. Aber der folgende Satz liefert einen Ansatzpunkt:

Sei $f(X) = X^n - a_1 X^{n-1} + a_2 X^{n-2} - + \dots + (-1)^n \cdot a_n \in K[X]$ ein separables Polynom. Schreibe $f(X) = \prod_{i=1}^n (X - \alpha_i)$ mit $\alpha_i \in \bar{K}$. Dann ist $L := K(\alpha_1, \dots, \alpha_n)$ ein Zerfällungskörper von f und $\Gamma := \mathrm{Gal}(L/K)$ seine Galoisgruppe. Diese ist eine Untergruppe von S_n via $\gamma(\alpha_i) = \alpha_{\gamma i}$ für alle $\gamma \in \Gamma$.

<u>Satz</u>: Setze $g := \prod_{\sigma \in S_n} \Big(Z - \underbrace{\sum_{i=1}^n \alpha_{\sigma i} Y_i}_{=: \, l_\sigma}\Big) \in L[Z, Y_1, \dots, Y_n]$ Hilfsvariablen!

(a) $g = G(Z, Y_1, \dots, Y_n, a_1, \dots, a_n)$ für ein nur von n abhängiges Polynom $G \in \mathbb{Z}[Z, Y_1, \dots, Y_n, S_1, \dots, S_n]$. Insbesondere hat g Koeffizienten in K.

(b) Sei $h \in K[Z, Y_1, \dots, Y_n]$ ein irreduzibler Faktor von g. Dann existiert $\sigma \in S_n$ so dass gilt

$$\{\tau \in S_n \mid h(Z, Y_{\tau 1}, \dots, Y_{\tau n}) = h\} = \sigma^{-1} \Gamma \sigma .$$

<u>Folge</u>: Sei K ein Körper, so dass ein Algorithmus existiert, Polynome in beliebig vielen Variablen über K in irreduzible Faktoren zu zerlegen. Dann existiert ein Algorithmus, der die Galoisgruppe jedes separablen Polynoms in $K[X]$ bestimmt.

<u>Bem.</u>: $K = \mathbb{Q}$ erfüllt die Voraussetzung (siehe Serie 13, Aufg. 8)

<u>Bem.</u>: Der Satz eignet sich nicht gut für effiziente Rechnungen, da der Umgang mit Polynomen in $n+1$ Variablen sehr aufwendig ist. In der Praxis tun es ad hoc Ansätze vom Typ

$$\prod_{S_n\text{-Konjugierte}} \left(Z - \left(\begin{smallmatrix}\text{etwas partiell} \\ \text{invariantes in } \alpha_1, \dots, \alpha_n\end{smallmatrix}\right)\right)$$

besser. Zum Beispiel $\prod_{i<j} (Z - \alpha_i - \alpha_j)$, etc. ...

Siehe auch unten.

Beweis des Satzes: (a) Setze

$$\tilde{G} := \prod_{\sigma\in S_n}\left(Z-\sum_{i=1}^{n} X_{\sigma i}\, Y_i\right) \in \mathbb{Z}[Z, Y_1,\dots,Y_n, X_1,\dots,X_n]$$

Offenbar ist dieses Polynom symmetrisch in $X_1,\dots,X_n$; folglich ist
$\tilde{G} = G(Z, Y_1,\dots,Y_n, S_1,\dots,S_n) \in \mathbb{Z}[Z, Y_1,\dots,Y_n, S_1,\dots,S_n]$,
wobei S_i das ite elementarsymmetrische Polynom in $X_1,\dots,X_n$ ist.
Damit ist

$$g = \tilde{G}(Z, Y_1,\dots,Y_n, \alpha_1,\dots,\alpha_n) = G(Z, Y_1,\dots,Y_n, a_1,\dots,a_n) \in K[Z, Y_1,\dots,Y_n].$$

(b) Zur Abkürzung setzen wir $l_\sigma := \sum_{i=1}^{n} \alpha_{\sigma i} \cdot Y_i$. Dann gilt

$$\forall \gamma\in\Gamma:\ \gamma(l_\sigma) = \sum_{i=1}^{n} \gamma(\alpha_{\sigma i})\, Y_i = \sum_{i=1}^{n} \alpha_{\gamma\sigma i}\, Y_i = l_{\gamma\sigma}, \text{ und}$$

(*) $$\forall \tau\in S_n:\ l_\sigma(Y_{\tau 1},\dots,Y_{\tau n}) = \sum \alpha_{\sigma i} Y_{\tau i} = \sum \alpha_{\sigma\tau^{-1} j}\, Y_j = l_{\sigma\tau^{-1}}.$$

Da h nichtkonstant ist, existiert $\sigma\in S_n$ mit $Z - l_\sigma \mid h$ in $L[Z, Y_1,\dots,Y_n]$. Es folgt $\forall\gamma\in\Gamma:\ Z - l_{\gamma\sigma} = \gamma(Z - l_\sigma) \mid \gamma(h) = h$.
Da die $l_{\gamma\sigma}$ paarweise verschiedene Nullstellen für Z in dem Integritätsbereich $L[Y_1,\dots,Y_n]$ sind, folgt $\prod_{\gamma\in\Gamma}(Z - l_{\gamma\sigma}) \mid h$.
Aber dieser Teiler ist nach Konstruktion Γ-invariant, hat also Koeffizienten in K, genau wie h. Folglich gilt diese Teilbarkeit schon in $K[Z, Y_1,\dots,Y_n]$. Da h irreduzibel ist, folgt Gleichheit, das heißt $h = \prod_{\gamma\in\Gamma}(Z - l_{\gamma\sigma})$.

Für jedes $\tau\in S_n$ gilt daher

$$h(Z, Y_{\tau 1},\dots,Y_{\tau n}) = \prod_{\gamma\in\Gamma}\left(Z - l_{\gamma\sigma}(Y_{\tau 1},\dots,Y_{\tau n})\right) \overset{(*)}{=} \prod_{\gamma\in\Gamma}(Z - l_{\gamma\sigma\tau^{-1}}).$$

Da aber die $l_{\sigma'}$ für $\sigma'\in S_n$ paarweise verschieden sind, ist dies $= h \iff \{\gamma\sigma\tau^{-1} \mid \gamma\in\Gamma\} = \{\gamma\sigma \mid \gamma\in\Gamma\}$
$\iff \Gamma\sigma\tau^{-1} = \Gamma\sigma \iff \Gamma\sigma = \Gamma\sigma\tau$
$\iff \tau \in \sigma^{-1}\Gamma\sigma$. qed.

Bem.: Der Beweis liefert auch die Produktzerlegung

$$g = \prod_{\sigma'\in S_n}(Z - l_{\sigma'}) = \prod_{[\tau]\in\sigma^{-1}\Gamma\sigma\backslash S_n}\ \prod_{\gamma\in\Gamma}(Z - l_{\gamma\sigma\tau^{-1}})$$

(**) $$= \prod_{[\tau]\in\sigma^{-1}\Gamma\sigma\backslash S_n} h(Z, Y_{\tau 1},\dots,Y_{\tau n})$$

Dabei sind die Faktoren irreduzibel in $K[Z, Y_1,\dots,Y_n]$ und paarweise inäquivalent.

Spezialfall: Sei $f(X) \in \mathbb{Z}[X]$ normiert reparabel vom Grad n mit Galoisgruppe $\Gamma \subset S_n$.

Satz: Sei p eine Primzahl, die die Diskriminante D_f nicht teilt. Sei $f \equiv \prod_{i=1}^{r} \bar{f}_i \pmod p$ Produkt irreduzibler Faktoren $\bar{f}_i \in \mathbb{F}_p[X]$ vom Grad n_i mit $\sum_{i=1}^{r} n_i = n$. Dann enthält Γ ein Element γ, das Produkt disjunkter n_i-Zyklen für $1 \le i \le r$ ist.

Beweis: Wegen $p \nmid D_f$ ist $\bar{f} := f \pmod p \in \mathbb{F}_p[X]$ wieder reparabel. Seien $\bar{\alpha}_1, \dots, \bar{\alpha}_n \in \overline{\mathbb{F}_p}$ seine Nullstellen und $\bar{\Gamma} := \mathrm{Gal}(\mathbb{F}_p(\bar{\alpha}_1, \dots, \bar{\alpha}_n)/\mathbb{F}_p) \subset S_n$ seine Galoisgruppe. Nach §6 ist $\bar{\Gamma}$ zyklisch mit $\bar{\sigma} := \mathrm{Frob}_p$ erzeugt. Dabei entsprechen die irreduziblen Faktoren $\bar{f}_i$ genau den Bahnen von $\bar{\sigma}$ auf $\{\bar{\alpha}_1, \dots, \bar{\alpha}_n\}$, also den Zyklen in einer disjunkten Zyklenzerlegung von $\bar{\sigma}$. Folglich ist $\bar{\sigma} \in S_n$ ein Element des gesuchten Typs!

Um zu zeigen, dass dieses schon in Γ auftritt, können wir versuchen, die α_i und die $\bar{\alpha}_i$ in die richtige Beziehung zu bringen. Dies würde bedeuten, die Restklassenabbildung $\mathbb{Z} \to \mathbb{F}_p$ auf Ringe algebraischer Zahlen zu verallgemeinern und den Zusammenhang mit der Galoisoperation zu bestimmen. Dies ist Gegenstand der algebraischen Zahlentheorie. Mit dem vorliegenden Satz kann man diese neuen Konzepte vermeiden (obwohl eigentlich erst sie die Sache wirklich erhellen ...).

Sei $g = h(t, \gamma_1, \dots, \gamma_n, a_1, \dots, a_n)$ und h ein irreduzibler Faktor von g in $\mathbb{Q}[t, \gamma_1, \dots, \gamma_n]$, wie im vorhergehenden Satz. Dann $\exists\, \sigma \in S_n$: $\mathrm{Stab}_{S_n}(h) = \sigma^{-1} \Gamma \sigma$.
Nun hat aber g Koeffizienten in $\mathbb{Z}$, und ist normiert in t. Wählen wir auch h normiert in t, so folgt nach Gauß (Teil B, §6), dass auch $h \in \mathbb{Z}[t, \gamma_1, \dots, \gamma_n]$ ist. Wir können daher beide Polynome modulo p reduzieren und erhalten: $\bar{h} := h \bmod p$ teilt $\bar{g} := g \bmod p$ in $\mathbb{F}_p[t, \gamma_1, \dots, \gamma_n]$.

Aber $\bar{g}$ ist das nach dem Satz zu $\bar{f} = f \bmod p$ assoziierte Hilfspolynom. Ist also $\bar{t} \in \mathbb{F}_p[z, \tau_1, \dots, \tau_n]$ ein irreduzibler Faktor von $\bar{h}$, so folgt: $\exists\, \bar{\sigma} \in S_n : \mathrm{Stab}_{S_n}(\bar{t}) = \bar{\sigma}^{-1} \bar{\Gamma} \bar{\sigma}$.

Nun liefert die Formel (**) nach Reduktion modulo p die Zerlegung

$$\bar{g} = \prod_{[\tau] \in \bar{\sigma}^{-1}\Gamma\sigma \backslash S_n} \bar{h}(z, \tau_{\tau 1}, \dots, \tau_{\tau n}).$$

Wenden wir nie anderenzeits auf $\bar{t}$ direkt über $\mathbb{F}_p$ an, so erhalten wir

$$\bar{g} = \prod_{[\tau] \in \bar{\sigma}^{-1}\bar{\Gamma}\bar{\sigma} \backslash S_n} \bar{t}(z, \tau_{\tau 1}, \dots, \tau_{\tau n}).$$

Dabei sind letztere Faktoren paarweise inäquivalente irreduzible in $\mathbb{F}_p[z, \tau_1, \dots, \tau_n]$. Damit sind die ersteren zwar möglicherweise reduzibel, aber immerhin paarweise teilerfremd. Wegen $\bar{t} \mid \bar{h}$ folgt also $\bar{t} \nmid \bar{h}(z, \tau_{\tau 1}, \dots, \tau_{\tau n})$ für alle $\tau \in S_n \setminus \bar{\sigma}^{-1}\Gamma\sigma$. Es gilt also:

$$\forall \tau \in S_n : \tau \in \bar{\sigma}^{-1}\bar{\Gamma}\bar{\sigma} \Rightarrow \bar{t} = \bar{t}(z, \tau_{\tau 1}, \dots, \tau_{\tau n}) \mid \bar{h}(z, \tau_{\tau 1}, \dots, \tau_{\tau n})$$
$$\overset{!}{\Rightarrow} \tau \in \bar{\sigma}^{-1}\Gamma\sigma.$$

Also haben wir $\bar{\sigma}^{-1}\bar{\Gamma}\bar{\sigma} \subset \bar{\sigma}^{-1}\Gamma\sigma$.

Folglich ist $\gamma := \sigma\bar{\sigma}^{-1} \cdot \bar{\gamma} \cdot (\sigma\bar{\sigma}^{-1})^{-1} \in \Gamma$ ein Element des gesuchten Typs.

qed

Beispiel: Die Galoisgruppe des Polynoms $f(X) := X^7+3X^2+5$ über $\mathbb{Q}$ ist ... S_7.

Beweis: $f \bmod 2 = X^7+X^2+1 = \underbrace{(X^2+X+1)}_{\text{irred.}} \cdot \underbrace{(X^5+X^4+X^2+X+1)}_{\text{irred.}}$

wie man durch probeweises Teilen durch alle irreduziblen Polynome in $\mathbb{F}_2[X]$ vom Grad ≤ 3 leicht feststellt. Da die Reduktion also weder separabel ist, wird die Voraussetzung des Satzes erfüllt. Also enthält die Galoisgruppe Γ von f ein Element der Form (2-Zykel)$\times$(5-Zykel) (disjunkt).

Analog findet man

$$f \bmod 3 = X^7-1 = \underbrace{(X-1)}_{\text{irred.}}\underbrace{(X^6+X^5+\ldots+X+1)}_{\text{irred.}}.$$

Also enthält Γ ein Element der Form (1-Zykel)$\times$(6-Zykel).

Aber: Die einzige Untergruppe $\Gamma < S_7$, die solche Elemente enthält, ist die S_7 selbst.

Denn: Γ hat unter jedem der beiden Elemente höchstens 2 Bahnen. Aber die Längen dieser Bahnen sind jeweils verschieden $\Rightarrow \Gamma$ hat nur eine Bahn. Also ist $7 = |\{1,\ldots,7\}|$ ein Teiler von $|\Gamma|$. Daher enthält Γ einen 7-Zykel. Außerdem ist die 5-te Potenz eines Elements der ersten Form eine Transposition. Schließlich weiß man, dass jeder 7-Zykel und jede Transposition die S_7 erzeugen. **qed**.

(**Bem**: Wegen des Elements vom zweiten Typ ist Γ sogar zweifach transitiv. Da es eine Transposition enthält, enthält es daher alle Transpositionen. Aber diese erzeugen die S_7.)