"GAGA B" — WiSe 2019/20

M. Geck, IAZ – Lehrstuhl für Algebra, Universität Stuttgart, Januar 2020

Diese Notizen enthalten einen Beweis der **Newton–Identitäten**, die im letzten Abschnitt der Vorlesung (über Invarianten endlicher Gruppen) benutzt wurden.

Wir betrachten den Polynomring $R[X]$ in einer Unbestimmten X über einem beliebigen kommutativen Ring R mit 1. Wir beginnen mit einer Vorbetrachtung zum Horner–Schema. Sei $0 \neq f \in R[X]$ ein Polynom vom Grad $n \geq 1$ und schreibe dies in der Form

$$f = \sum_{d=0}^{n} a_d X^{n-d} = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \qquad \text{mit } a_d \in R \text{ und } a_0 \neq 0.$$

Sei $c \in R$ eine Nullstelle von f. Wir definieren Koeffizienten $b_d \in R$ wie folgt ("Horner-Schema"):

$$\begin{aligned}
b_0 &:= a_0,\\
b_1 &:= a_0c + a_1,\\
b_2 &:= a_0c^2 + a_1c + a_2,\\
b_3 &:= a_0c^3 + a_1c^2 + a_2c + a_3,\\
&\ \vdots\\
b_{n-1} &:= a_0c^{n-1} + a_1c^{n-2} + \ldots + a_{n-2}c + a_{n-1}.
\end{aligned}$$

Es ist also $b_d - cb_{d-1} = a_d$ für $1 \leq d \leq n-1$. Dann gilt $f = (X-c)g$ mit dem Polynom

$$g := \sum_{d=0}^{n-1} b_d X^{n-1-d} = b_0X^{n-1} + b_1X^{n-2} + \ldots + b_{n-2}X + b_{n-1} \in R[X].$$

[Dies folgt durch einfaches Nachrechnen:

$$\begin{aligned}
(X-c)g = Xg - cg &= \sum_{d=0}^{n-1} b_dX^{n-d} - \sum_{d=0}^{n-1} cb_dX^{n-1-d} = \sum_{d=0}^{n-1} b_dX^{n-d} - \sum_{d=1}^{n} cb_{d-1}X^{n-d}\\
&= b_0X^n + \Big(\sum_{d=1}^{n-1} \underbrace{(b_d - cb_{d-1})X^{n-d}}_{=a_d}\Big) - cb_{n-1} = a_0X^n + \Big(\sum_{d=1}^{n-1} a_dX^{n-d}\Big) - cb_{n-1}.
\end{aligned}$$

Schließlich beachte $cb_{n-1} = a_0c^n + a_1c^{n-1} + \ldots + a_{n-1}c = f(c) - a_n = -a_n$, also gilt $(X-c)g = f$. $\Box$]

Seien nun $c_1, \ldots, c_n \in R$ fest und definiere

$$f_0 := (X - c_1)(X - c_2) \cdots (X - c_n) \in R[X].$$

Dann hat f_0 den Grad n und ist normiert. Wie oben schreiben wir $f_0 = \sum_{d=0}^{n} a_dX^{n-d}$ mit $a_d \in R$ und $a_0 = 1$. Da jedes c_i eine Nullstelle von f_0 ist, gibt es Polynome $g^{(i)} \in R[X]$ mit $f_0 = (X-c_i)g^{(i)}$, wobei $g^{(i)}$ den Grad $n-1$ hat und ebenfalls normiert ist. Wir schreiben

$$g^{(i)} = \sum_{d=0}^{n-1} b_d^{(i)} X^{n-1-d} \qquad \text{mit} \qquad b_d^{(i)} = \sum_{j=0}^{d} a_{d-j}c_i^j = a_0c_i^d + \ldots + a_{d-1}c_i + a_d \qquad \text{(siehe oben).}$$

Damit erhalten wir

$$(*) \quad \sum_{i=1}^{n} g^{(i)} = \sum_{i=1}^{n}\sum_{d=0}^{n-1} b_d^{(i)} X^{n-1-d} = \sum_{d=0}^{n-1}\Big(\sum_{i=1}^{n}\sum_{j=0}^{d} a_{d-j}c_i^j\Big)X^{n-1-d} = \sum_{d=0}^{n-1}\sum_{j=0}^{d} a_{d-j}\Big(\sum_{i=1}^{n} c_i^j\Big)X^{n-1-d}$$

Betrachten wir andererseits die formale Ableitung von Polynomen in $R[X]$ bezüglich X; bezeichnen wir diese mit $D\colon R[X] \to R[X]$. Dann ist D linear, es gilt $D(1) = 0$, $D(X^m) = mX^{m-1}$ für alle

$m \geq 1$ und es gilt die Produkregel $D(f_1 f_2) = f_1 D(f_2) + f_1 D(f_2)$ für alle $f_1, f_2 \in R[X]$. Mit einer leichten Induktion nach $m \in N$ zeigt man dann (Beweis als Übung):

$$D(f_1 f_2 \cdots f_m) = \sum_{i=1}^{m} f_1 \cdots f_{i-1} D(f_i) f_{i+1} \cdots f_m \qquad \text{für } f_1, \ldots, f_m \in R[X].$$

Angewandt auf $f_0 = \sum_{d=0}^{n} a_d X^{n-d} = (X - c_1)(X - c_2) \cdots (X - c_n)$ erhalten wir also die Identitäten

$$\begin{aligned} D(f_0) &= \sum_{d=0}^{n-1} (n-d) a_d X^{n-1-d} \\ &= \sum_{i=1}^{n} (x - c_1) \cdots (X - c_{i-1})(X - c_{i+1}) \cdots (X - c_n) = \sum_{i=1}^{n} \frac{f_0}{X - c_i} = \sum_{i=1}^{n} g^{(i)}. \end{aligned}$$

Vergleichen wir die Koeffizienten von X^{n-1-d}, so erhalten wir mit $(*)$:

$$\sum_{j=0}^{d} a_{d-j} \Big(\sum_{i=1}^{n} c_i^j \Big) = (n-d) a_d \qquad \text{für } 0 \leq d \leq n-1.$$

Definiere nun die Potenzsumme $p_j := \sum_{i=1}^{n} c_i^j$ für $j = 0, 1, 2, \ldots$ (Für $j = 0$ ist also $p_0 = n$.)

Dann schreibt sich obige Gleichung als $n a_d + \sum_{j=1}^{d} a_{d-j} p_j = (n-d) a_d$. Also erhalten wir schließlich

$$\boxed{d a_d + p_1 a_{d-1} + p_2 a_{d-2} + \ldots + p_d a_0 = 0 \qquad \text{für } 1 \leq d \leq n.}$$

Zur Erinnerung: Hier sind die a_d die Koeffizienten von $f_0 = (X - c_1)(X - c_2) \cdots (X - c_n)$. D.h.,

$$a_0 = 1 \qquad \text{und} \qquad a_d = (-1)^d \sum_{1 \leq i_1 < \ldots < i_d \leq n} c_{i_1} \cdots c_{i_d} \qquad \text{für } 1 \leq d \leq n.$$

Sei nun R der Polynomring $R = \mathbb{Q}[X_1, \ldots, X_n]$ in n Unbestimmten $X_1, \ldots, X_n$. Wir definieren $\sigma_0 := 1$, $\pi_0 := n$ sowie für alle $d \geq 1$:

$$\sigma_d := \sum_{1 \leq i_1 < \ldots < i_d \leq n} X_{i_1} \cdots X_{i_d} \qquad \text{“}d\text{-tes elementar-symmetrisches Polynom”},$$

$$\pi_d := \sum_{1 \leq i \leq n} X_i^d \qquad \text{“}d\text{-te Newton-Potenzsumme”}.$$

Die obigen Rechnungen (mit $c_i = X_i$ für $1 \leq i \leq n$) zeigen also die folgenden Newton-Identitäten:

$$\boxed{(-1)^d d \sigma_d + (-1)^{d-1} \pi_1 \sigma_{d-1} + (-1)^{d-2} \pi_2 \sigma_{d-2} + \ldots + \pi_d \sigma_0 = 0 \qquad \text{für } 1 \leq d \leq n.}$$

Mit Hilfe dieser Gleichungen und einer Rekursion lässt sich jedes σ_d (für $1 \leq d \leq n$) als Polynom in $\pi_1, \ldots, \pi_d$ schreiben, und umgekehrt.

Eine Anwendung. Sei $A \in M_n(\mathbb{C})$. Dann lässt sich das charakteristische Polynom $\chi_A \in \mathbb{C}[X]$ von A aus den Werten $\mathrm{Spur}(A^d)$ für $1 \leq d \leq n$ berechnen.

[Beweis: Da $\mathbb{C}$ algebraisch abgeschlossen ist, gibt es $\lambda_i \in \mathbb{C}$ mit $\chi_A = (-1)^n (X - \lambda_1) \cdots (X - \lambda_n)$. (Die λ_i müssen nicht verschieden sein.) Dann ist $\chi_A = \sum_{d=0}^{n} a_d X^{n-d}$ mit $a_d = (-1)^{n+d} \sigma_d(\lambda_1, \ldots, \lambda_n)$. Weiterhin gibt es eine invertierbare Matrix $T \in M_n(\mathbb{C})$, so dass $T^{-1} A T$ eine obere Dreiecksmatrix mit $\lambda_1, \ldots, \lambda_n$ auf der Diagonalen ist. Für $1 \leq d \leq n$ ist dann $(T^{-1} A T)^d$ ebenfalls eine obere Dreiecksmatrix, mit $\lambda_1^d, \ldots, \lambda_n^d$ auf der Diagonalen. Es folgt $\mathrm{Spur}(A^d) = \mathrm{Spur}(T^{-1} A^d T) = \mathrm{Spur}\big((T^{-1} A T)^d\big) = \lambda_1^d + \ldots + \lambda_n^d = \pi_d(\lambda_1, \ldots, \lambda_n)$. Mit Hilfe der Newton-Identitäten können also die Koeffzienten von χ_A als Polynom in den Werten $\mathrm{Spur}(A^d)$ für $1 \leq d \leq n$ geschrieben werden. $\square$]