Die Kommutativität endlicher Schiefkörper

Lukas-Fabian Moser, SS 2013

Es sei R ein endlicher Schiefkörper und $G := R \setminus \{0\}$ die Gruppe seiner invertierbaren Elemente. Wir betrachten die Klassengleichung für diese Gruppe (also die Bahnengleichung für ihre Operation auf sich selbst durch Konjugation), welche lautet

$$|G| = |Z(G)| + \sum_{i=1}^{t} \frac{|G|}{|C_G(r_i)|},$$

wobei $r_1, \ldots, r_t$ ein Repräsentantensystem der Konjugationsklassen der Größe $\geqslant 2$ ist.

Die Ausdrücke in dieser Gleichung, die sich ja für jede endliche Gruppe aufstellen läßt, kann man nun genauer bestimmen, wenn man ausnutzt, daß G die Einheitengruppe des endlichen Schiefkörpers R ist:

i) Das Zentrum $Z(G)$ von G ist fast identisch mit dem Zentrum K des Schiefkörpers R, das definiert ist als

$$K = \{x \in R \,|\, rx = xr \text{ für alle } r \in R\}.$$

Denn es ist ja

$$Z(G) = \{0 \neq x \in R \,|\, rx = xr \text{ für alle } 0 \neq r \in R\}.$$

Da die Bedingung $rx = xr$ für $r = 0$ sowieso immer erfüllt ist, sieht man, daß $K = Z(G) \cup \{0\}$ ist. Unsere Klassengleichung lautet also nun

$$|R| - 1 = |K| - 1 + \sum_{i=1}^{t} \frac{|R| - 1}{|C_G(r_i)|},$$

ii) Die Menge K ist ein Unterschiefkörper von R (!), der außerdem nach seiner Konstruktion kommutativ ist – also ist K ein endlicher Körper. Setzen wir $q := |K|$ (dies ist stets eine Primzahlpotenz, was aber im Folgenden nicht benötigt wird). Da man R als Vektorraum über K auffassen kann, folgt $|R| = q^n$, wobei $n = \dim_K R$ ist.

iii) Für jedes i ist die Menge $C_G(r_i)$ definiert als

$$C_G(r_i) = \{0 \neq x \in R \,|\, r_i x = x r_i\}\,.$$

Diese ist fast identisch mit der Menge

$$C_R(r_i) := \{x \in R \,|\, r_i x = x r_i\}\,,$$

denn es ist sicher $C_R(r_i) = C_G(r_i) \cup \{0\}$. Aber $C_R(r_i)$ ist ein K-Untervektorraum von R, also folgt $|C_R(r_i)| = q^{n_i}$ mit $n_i = \dim_K C_R(r_i)$ und damit $|C_G(r_i)| = q^{n_i} - 1$.

Setzt man alle diese Berechnungen in unsere Klassengleichung ein, so erhält sie die Form

$$q^n - 1 = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{n_i} - 1}.$$

Dabei gilt außerdem $n_i < n$, da das Summenzeichen in der Klassengleichung stets nur Summanden größer als 1 umfaßt. Nach Konstruktion sind außerdem alle Summanden ganzzahlig.

Man kann noch einen weiteren Zusammenhang zwischen den Summanden dieser Gleichung feststellen:

Lemma. *Sind q, n, m natürliche Zahlen, $q \geqslant 2$ und $n, m \geqslant 1$, so ist $q^m - 1 \mid q^n - 1$ äquivalent zu $m \mid n$.*[1]

Beweis des Lemmas. Im Ring $\mathbb{Z}/(q^m - 1)$ ist q invertierbar, und in der Einheitengruppe $(\mathbb{Z}/(q^m - 1))^*$ hat $\overline{q}$ die Ordnung m. Nun gilt $q^m - 1 \mid q^n - 1$ genau dann, wenn $\overline{q}^n = \overline{1}$ ist, was äquivalent ist zu $m = \operatorname{ord} \overline{q} \mid n$.[2] □

Der Satz von Wedderburn über die Kommutativität endlicher Schiefkörper ist also bewiesen, wenn wir zeigen können:

Satz (Wedderburn–Dickson, 1905)**.** *Ist $q \geqslant 2$ eine natürliche Zahl, ist $n \geqslant 1$, und sind $n_1, \ldots, n_t$ echte Teiler von n mit*

$$q^n - 1 = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{n_i} - 1},$$

so ist $n = 1$ und $t = 0$.

[1] Das Lemma liefert übrigens einen rein arithmetischen Beleg für eine Aussage über endliche Körper: Ein Körper mit p^n Elementen kann nur dann einen Unterkörper mit p^m Elementen haben, wenn $m \mid n$ gilt (denn es muß ja die $(p^m - 1)$-elementige Einheitengruppe des kleinen Körpers eine Untergruppe der $(p^n - 1)$-elementigen Einheitengruppe des großen sein). (Der in der Algebra übliche Beweis geht so: Der große Körper ist ein Vektorraum über dem kleinen; ist seine Dimension d, so folgt $p^n = (p^m)^d = p^{md}$, also $n = md$.)

[2] Ein direkter Beweis für die Richtung „$\Longleftarrow$“: Gilt $m \mid n$, so kann man, indem man q durch q^m ersetzt, annehmen, daß $m = 1$ ist. Aber dann ist

$$q^n - 1 = (q - 1)(1 + q + q^2 + \cdots + q^{d-1})$$

nach der geometrischen Summenformel ein Vielfaches von $q - 1$.

Beweis (Witt, 1931). Für jeden echten Teiler d von n ist Φ_n ein Faktor des (ganzzahligen) Polynoms

$$\frac{X^n - 1}{X^d - 1} = \prod_{\substack{m|n \\ m\nmid d}} \Phi_m,$$

woraus durch Einsetzen von $X = q$ folgt

$$\Phi_n(q) \mid \frac{q^n - 1}{q^d - 1}.$$

In der Ausgangsgleichung sind also die linke Seite und alle Summanden im Summenzeichen durch $\Phi_n(q)$ teilbar, und das erzwingt auch $\Phi_n(q) \mid q - 1$.

Andererseits ist

$$\Phi_n(q) = \prod_{\zeta} (q - \zeta),$$

wobei sich das Produkt über alle primitiven n-ten Einheitswurzeln erstreckt. Da q aber insbesondere eine reelle Zahl $\geqslant 1$ ist, ist $|q - \zeta| > |q - 1|$ für jede primitive n-te Einheitswurzel $\zeta \neq 1$ (das sieht man am einfachsten geometrisch). Wenn es also eine primitive n-te Einheitswurzel $\zeta \neq 1$ gibt, so folgt

$$|\Phi_n(q)| = \prod_{\zeta} |q - \zeta| > \prod_{\zeta} |q - 1| > q - 1$$

im Widerspruch zu $\Phi_n(q) \mid q - 1$. Also ist $\zeta = 1$ die einzige primitive n-te Einheitswurzel, und das heißt $n = 1$ (und damit automatisch $t = 0$). □