Burnsides $p^a q^b$-Satz

Uli Wagner

6. Dezember 1999

1 Vorgeschichte

In den Zeiten vor Abel und Galois war es eines der Hauptanliegen der Algebraiker, "Formeln" für die Lösungen von Polynomgleichungen zu finden, wobei diese Formeln mittels rationaler Operationen und Wurzeln aus den Koeffizienten der jewiligen Gleichung aufgebaut sein sollten. Präzisiert man dieses Problem, so gelangt man zu folgender

Definition 1.1. Sei E ein Erweiterungskörper von F. Man spricht von einer **Radikal-Erweiterung**, falls $E = F(u_1, \ldots, u_n)$ und jeweils

$$u_i^{m_i} \in F(u_1, \ldots, u_{i-1})$$

für ein $m_i \geq 1$. Ist ferner ein Polynom $f \in F[x]$ gegeben, so heißt die Gleichung $f(x) = 0$ **lösbar durch Radikale**, falls der Zerfällungskörper[1] E von f über F eine Radikalerweiterung ist.

Eines der Glanzstücke von Évariste Galois ist die folgende Charakterisierung von Radikalerweiterungen:

Satz 1.2. *Sei $f \in F[x]$ vom Grade n, $\mathrm{char}(F) = 0$. Dann ist*[2]

$$f(x) = 0 \text{ lösbar durch Radikale} \iff \mathrm{Gal}(f/F) \text{ ist } \textbf{auflösbar} \tag{1}$$

im Sinne der nachstehenden Definition. [3]

(Für den Beweis dieses Satzes verweise ich auf [1].)

Definition 1.3. Eine Gruppe G heißt **auflösbar**, falls es eine *Normalreihe*

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = \{1\}$$

gibt, so daß alle Quotienten G_i/G_{i+1} abelsch sind.[4]

[1] Zur Erinnerung: Der Zerfällungskörper von f über F entsteht grob gesagt dadurch, daß man alle Wurzeln von f zu F hinzu adjungiert. Mit anderen Worten: Er ist der (bis auf Isomorphie eindeutige) inklusionsminimale Erweiterungskörper von F, über dem f in lineare Faktoren zerfällt.

[2] Hierbei gilt "$\Rightarrow$" in jeder Charakteristik, und "$\Leftarrow$" allgemeiner im Fall $\mathrm{char}(F) \nmid n!$.

[3] $\mathrm{Gal}(f/F)$ bezeichnet hierbei die Galois-Gruppe des Zerfällungskörpers E von f über F, d.h. die Gruppe aller Automorphismen von E, die F punktweise fixieren.

[4] Achtung! Es wird keineswegs $G_i \trianglelefteq G$ für alle i vorausgesetzt.

Beispiele 1.4. 1. Die symmetrische Gruppe S_n ist *nicht auflösbar*, falls $n \geq 5$ (der Grund ist im wesentlichen, daß A_n dann einfach und nicht abelsch ist). Mit etwas zusätzlichem Aufwand folgt daraus der Satz von Abel, daß es keine allgemeine Lösungsformel für Gleichungen vom Grade ≥ 5 gibt.

2. Trivialerweise ist jede abelsche Gruppe auflösbar.

Hier sind ein paar praktische Lemmas, um weitere Beispiele von auflösbaren Gruppen zu finden.

Lemma 1.5. *Eine Gruppe G ist genau dann auflösbar, wenn die induktiv durch $G^{(0)} := G$ und $G^{(i+1)} := \left(G^{(i)}\right)'$ definierte* ***Kommutatorreihe*** *$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \ldots$ terminiert, d.h. wenn $G^{(n)} = \{1\}$ für ein $n \in \mathbb{N}$. Dabei ist H' die* ***Kommutatorgruppe*** *einer Gruppe H.*[5]

Beweis. Terminiert die Kommutatorreihe, so stellt sie eine Normalreihe mit abelschen Quotienten dar. Ist umgekehrt $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = \{1\}$ eine Normalreihe mit abelschen Quotienten, so sieht man leicht durch Induktion über i, daß $G^{(i)} \leq G_i$ für alle i, also insbesondere $G^{(n)} = \{1\}$. □

Lemma 1.6. *Untergruppen und homomorphe Bilder von auflösbaren Gruppen sind wieder auflösbar.*

Beweis. Die Normalreihe $G = G_0 \trianglerighteq \ldots \trianglerighteq G_n = \{1\}$ bezeuge, daß G auflösbar ist, d.h. G_i/G_{i+1} abelsch. Ist $H \leq G$ bzw. $f : G \to B$ ein *surjektiver* Gruppenhomomorphismus, so werden durch $H_i := H \cap G_i$ bzw. $B_i := f[G_i]$ Normalreihen mit abelschen Quotienten definiert. □

Eine Art Umkehrung:

Lemma 1.7. *Ist $N \trianglelefteq G$, und sind sowohl N als auch G/N auflösbar, so ist auch G auflösbar.*

Beweis. Zunächst bemerken wir, daß aufgrund des Korrespondenzsatzes (auch Vierter Isomorphiesatz genannt) die Untergruppen von G/N von der Form H/N sind, wobei $N \leq H \leq G$; dabei ist $H/N \trianglelefteq G/N \iff H \trianglelefteq G$. Seien nun $N = N_0 \trianglerighteq \ldots \trianglerighteq N_k = \{1\}$ und $G/N = G_0/N \trianglerighteq G_1/N \trianglerighteq \ldots \trianglerighteq G_n/N = N/N$ Normalreihen mit abelschen Koeffizienten. Wir setzen diese einfach zusammen:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_n = N = N_0 \trianglerighteq N_1 \trianglerighteq \ldots \trianglerighteq N_k = \{1\}\,.$$

Dabei sorgt der Dritte Isomorphiesatz dafür, daß alle Quotienten abelsch sind. □

[5] Dies ist die von allen Elementen der Form $[a, b] := aba^{-1}b^{-1}$ $(a, b \in H)$ erzeugte Untergruppe; sie hat einige nützliche Eigenschaften:

1. $H' \trianglelefteq H$;
2. H/H' ist abelsch.
3. Ist N ein Normalteiler von H mit H/N abelsch, so gilt $H' \leq N$.

Als Anwendung sehen wir, daß alle p-Gruppen (Gruppen der Ordung p^n), p prim, auflösbar sind: Denn ist G derart, so entweder G abelsch, oder aber das Zentrum $Z(G)$ ist ein nichttrivialer Normalteiler; dann aber sind induktiv sowohl $Z(G)$ als auch $G/Z(G)$ auflösbar (beides sind p-Gruppen kleinerer Ordnung), also auch G.

Der Satz von Burnside ist eine Verallgemeinerung dieser Beobachtung auf den Fall von zwei Primfaktoren. Zunächst aber möchte ich die für den Beweis notwendigen Zutaten zusammentragen.

2 Hilfsmittel

Es sei G eine Gruppe mit $|G| = p^n m$, p prim und $p \nmid m$. Eine **p-Sylow-Untergruppe** von G ist eine Untergruppe $P \leq G$ der Ordnung $|P| = p^n$. Die Menge der p-Sylow-UG von G wird mit $\mathrm{Syl}_p(G)$ bezeichnet.

Satz 2.1 (Die Sylow-Sätze). *1. $\mathrm{Syl}_p(G) \neq \emptyset$.*

2. Ist $P \in \mathrm{Syl}_p(G)$ und ferner $Q \leq G$, $|Q| = p^k$ für ein $k \leq n$, so existiert ein $g \in G$ mit $Q \leq gPg^{-1}$. Insbesondere sind alle p-Sylow-Untergruppen zueinander konjugiert.

3. Es gilt $s := \left|\mathrm{Syl}_p(G)\right| = [G : N_G(P)]$ für jedes $P \in \mathrm{Syl}_p(G)$. Somit gilt $s \mid m$ und außerdem $s \equiv 1 \mod p$.

Ein Beweis findet sich etwa in [1]. Desweiteren werden wir einige im Seminar erarbeitete Resultate benötigen:

Notiz 2.2. Ist ρ eine komplexe Darstellung einer endlichen Gruppe G, so gilt $\rho(g)^{|G|} = I$ für alle $g \in G$; insbesondere sind alle Eigenwerte von $\rho(g)$ gewisse Einheitswurzeln. Ist somit n der Grad von ρ und χ der zugehörige Charakter, so gilt $|\chi(g)| \leq n$ für alle g, mit "=" genau dann, wenn $\rho(g) = \omega I$ für eine $|G|$-te Einheitswurzel ω. Insbesondere ist $Z(\chi) := \{g \in G \mid |\chi(g)| = n\} \trianglelefteq G$.

Notation 2.3. Wenn im folgenden von einer Gruppe mit Namen G die Rede ist, so bezeichnen immer

- $\rho_1, \ldots, \rho_r$ die *irreduziblen* Darstellungen von G,
- $n_1, \ldots, n_r$ deren Grade (also $\sum_i n_i^2 = |G|$),
- $\chi_1, \ldots, \chi_r$ die entsprechenden Charaktere; ferner seien
- $C_1, \ldots, C_r$ die Konjugiertenclassen von G.

Außerdem sei $\mathcal{C}\ell_G(a) := \{gag^{-1} \mid g \in G\}$ die Konjugiertenklasse von $a \in G$. Es sei daran erinnert, daß Charaktere Klassenfunktionen sind, d.h. konstant auf Konjugiertenklassen. Ich werde also ohne größere Scheu $\chi(C_i)$ schreiben, womit dann $\chi(g)$ gemeint ist für ein beliebiges $g \in C_i$.

Nach Notiz 2.2 ist $\chi(C_i)$ stets eine algebraisch ganze Zahl, d.h. Nullstelle eines normierten Polynoms mit ganzzahligen Koeffizienten. Der Ring der algebraisch ganzen Zahlen wird mit $\mathcal{A}$ bezeichnet; es sei daran erinnert, daß $\mathcal{A} \cap \mathbb{Q} = \mathbb{Z}$.

Ferner haben wir gesehen, daß

$$\omega_{\chi_j}(C_i) := \frac{|C_i|\,\chi_j(C_i)}{n_j}$$

immer eine algebraisch ganze Zahl ist.

Satz 2.4 (Orthogonalitätsrelation II). *Seien $a, b \in G$. Dann gilt*

$$\sum_{i=1}^{r} \chi_i(a)\overline{\chi_i(b)} = \begin{cases} \frac{|G|}{|\mathcal{C}\ell_G(a)|}, & \textit{falls } b \in \mathcal{C}\ell_G(a), \\ 0 & \textit{sonst.} \end{cases} \qquad \text{(OR II)}$$

3 Der Satz von Burnside

Satz 3.1. *Ist $|G| = p^a q^b$ mit p und q prim, so ist G auflösbar.*

Der hier präsentierte Beweis folgt [2] und basiert hauptsächlich auf den beiden folgenden Lemmas:

Lemma 3.2. *Es seien χ ein irreduzibler Charakter von G vom Grad $n = \chi(1)$ und C eine Konjugiertenklasse von G, so daß $|C|$ und n* relativ koprim *sind. Dann gilt*

$$\begin{array}{ll} \textit{entweder} & C \subseteq Z(\chi), \ \textit{d.h.}\ |\chi(C)| = n \\ \textit{oder} & \chi(G) = 0\,. \end{array}$$

Beweis. Wie oben angemerkt ist $\omega_\chi(C) = \frac{|C|\chi(C)}{n}$ eine algebraisch ganze Zahl. Nach Voraussetzung existieren ganze Zahlen k, l mit $k\,|C| + ln = 1$; wegen

$$\begin{aligned} k\omega_\chi(C) &= \frac{k\,|C|\,\chi(C)}{n} \\ &= \frac{\chi(C)}{n} + l\chi(C) \end{aligned}$$

ist somit auch

$$a := \frac{\chi(C)}{n}$$

eine algebraisch ganze Zahl.

Nun brauchen wir ein wenig Galois-Theorie. Es sei $K := \mathbb{Q}(\zeta)$ der $|G|$-te Kreisteilungskörper, d.h. ζ eine primitive $|G|$-te Einheitswurzel.

Fakt 3.3. *$K \supseteq \mathbb{Q}$ ist eine Galois-Erweiterung, d.h. wird $u \in K$ von allen $\sigma \in \Gamma := \mathrm{Gal}(K/\mathbb{Q})$ auf sich selbst abgebildet, so gilt $u \in \mathbb{Q}$. Desweiteren ist Γ isomorph zur multiplikativen Gruppe der primitiven $|G|$-ten Einheitswurzeln.*

Ist nun $\sigma \in \Gamma$, so bildet σ Einheitswurzeln wieder auf ebensolche ab, folglich ist auch $\sigma(\chi(C))$ wieder eine Summe von Einheitswurzeln; es gilt $|\chi(C)| = n \iff \chi(C) = \omega I$ für ein $\omega \iff \sigma(\chi(C)) = \sigma(\omega)I \iff |\sigma(\chi(C))| = n$. Ferner ist $\sigma(a)$ wieder eine algebraisch ganze Zahl, in der Tat Wurzel desselben Polynoms wie a, da σ die ganzzahligen Koeffizienten fixiert.

Betrachte nun

$$N := \prod_{\sigma \in \Gamma} \sigma(a)\,.$$

Es gelten: $N \in \mathcal{A}$, $|N| \leq 1$, $N \in \mathbb{Q}$, da N von allen $\sigma \in \Gamma$ fixiert wird. Folglich gilt $|N| = 0$ oder $|N| = 1$, was wegen $|\chi(C)| = n \iff |\sigma(\chi(C))| = n$ auf die zu beweisende Aussage hinausläuft. □

Lemma 3.4. *Sei G eine endliche,* nicht abelsche *Gruppe. Hat G eine Konjugiertenklasse C mit $|C| = q^k$ für eine Primzahl q und ein $k > 0$, so ist G nicht einfach (d.h. G hat einen nicht-trivialen Normalteiler).*

Beweis. Um zu einem Widerspruch zu gelangen, nehmen wir an, daß G doch einfach ist. Seien ρ_i, n_i, χ_i und C_i wie oben angegeben. O.B.d.A. sei χ_1 die triviale Darstellung. Da nun q ein Teiler von

$$|G| = 1 + \sum_{i=2}^{r} n_i^2\,,$$

gibt es ein $j \geq 2$ mit $q \nmid n_j$, also n_j und $|C|$relativ koprim. Nach Lemma 3.2 gilt für jedes solche j entweder $\chi_j(C) = 0$ oder $C \subseteq Z(\chi_j) = \{g \in G \mid |\chi_j(g)| = n\}$. Die zweite Möglichkeit ist allerdings ausgeschlossen: Sonst wäre nach Notiz 2.2 $\{1\} \neq Z(\chi_j) \trianglelefteq G$, also wegen Einfachheit $Z(\chi_j) = G$. Da ferner wegen $\rho_j \neq 1$ $\ker(\rho_j) \neq G$, also $\ker(\rho_j) = \{1\}$, gälte dann $G = Z(\chi_j)/\ker(\rho_j)$. Letzterer Quotient ist aber isomorph zu einer Untergruppe der $|G|$-ten Einheitswurzeln, also zyklisch; somit wäre G abelsch, ein Widerspruch.

Folglich gilt $\chi_j(C) = 0$ für alle $j \geq 2$ mit $q \nmid n_j$. Dann folgt mit (OR II)

$$\begin{aligned} 0 &= \sum_{i=1}^{r} \underbrace{\overline{\chi_i(1)}}_{=n_i} \chi_i(C) \\ &= 1 + \sum_{q \mid n_i} n_i \chi_i(C) + 0\,, \end{aligned}$$

also

$$\frac{1}{q} = -\sum_{q \mid n_i} \underbrace{\frac{n_i}{q}}_{\in \mathbb{Z}} \underbrace{\chi_i(C)}_{\in \mathcal{A}} \in \mathcal{A} \cap \mathbb{Q},$$

im Widerspruch zu der Tatsache, daß $\mathcal{A} \cap \mathbb{Q}$. □

Beweis des Satzes. Per Induktion über die Gruppenordnung genügt es nach Lemma 1.7, einen nichttrivialen Normalteiler von G zu finden. Da abelsche Gruppen ohnehin auflösbar sind, dürfen wir davon ausgehen, daß G nicht abelsch ist. Sei nun $P \in \mathrm{Syl}_p(G)$, d.h. $|P| = p^a$. Nach der Klassengleichung ist $Z(P) \neq \{1\}$. Ist $1 \neq z \in Z(P)$, so ist der Zentralisator $C_G(z) \geq P$, also ist $|\mathcal{C}\ell_G(z)| = [G : C_G(z)]$ eine Potenz q^k. Der Fall $k = 0$ ist trivial, denn dann ist z zentral in G, und $1 \neq \langle z \rangle \lhd G$ wie gewünscht; ist aber $k \geq 1$, so liefert Lemma 3.4 den gesuchten nichttrivialen Normalteiler. □

Literatur

[1] Thomas W. Hungerford. *Algebra.* Springer-Verlag, Berlin, 1980.

[2] Nathan Jacobson. *Basic Algebra II.* W.H. Freeman, New York, 1989.