Burnsides p^aq^b-Satz

von Andreas Klöckner

Ein Vortrag im Seminar "Darstellungstheorie endlicher Gruppen" von
Dr. S. Kühnlein und Prof. Dr. C.-G. Schmidt

28. Mai 2003

Inhaltsverzeichnis

1 Einführung

Im Rahmen dieses Vortrags werden wir die Struktur derjenigen endlichen Gruppen klären, deren Ordnung von höchstens zwei Primzahlen geteilt wird. Zu diesem Zweck benötigen wir einiges an Theorie. Zunächst werden wir uns mit dem Begriff der ganzalgebraischen Zahlen auseinandersetzen, dann ein zentrales Lemma beweisen, das sich mit so etwas wie "arithmetischen Mitteln" von Einheitswurzeln beschäftigt. Wir bauen ein wenig auf den Resultaten der vergangenen Vorträge auf und werden einen Satz beweisen, der innerhalb der Charaktertheorie schon recht tief liegt. Schließlich nähern wir uns über mehrere Lemmata unserem Hauptergebnis.

Dieser Vortrag basiert auf [Col90], [Neu92], [JL93] und [Ser77]. Diese Ausarbeitung mag manchem, der sich durch sie hindurchwühlt, sehr ausführlich erscheinen, dies erwuchs aus meinem Wunsch, mir selber keine Frage offen zu lassen. Jeden, der sich gelangweilt fühlt, bitte ich ausführlichst um Entschuldigung.

2 Vorbereitungen

2.1 Ganzalgebraische Zahlen

Im Folgenden sei stets mit dem Begriff "Ring" ein kommutativer Ring mit 1 gemeint.

Definition 2.1. *Sei $A \subset B$ eine Ringerweiterung. Ein Element $b \in B$ heißt ganzalgebraisch über A, falls es Nullstelle eines normierten Polynoms in $A[X]$ ist, d.h.*

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0 \quad (n \geqslant 1).$$

mit $a_i \in A$.

Es wäre natürlich wünschenswert, dass das Produkt und die Summe zweier ganzalgebraischer Zahlen wieder ganzalgebraisch sind. Das ist tatsächlich so, aber dieses Resultat fällt uns leider nicht direkt in den Schoß.

Um vorab ein wenig klarer werden zu lassen, was für Gebilde diese ganzalgebraischen Zahlen sind, betrachten wir diese Beispiele:

- A ist über sich selbst ganzalgebraisch: Jedes $a \in A$ ist Nullstelle der Gleichung $X - a = 0$.
- n-te Einheitswurzeln erfüllen die Gleichung $X^n - 1 = 0$ und sind somit ganzalgebraisch über $\mathbb{Z}$. Damit erhalten wir recht einfach, unter Benutzung der noch zu beweisenden Abgeschlossenheit bzgl. der Addition:

  Folgerung 2.2. *Sei $\chi: G \to \mathbb{C}$ ein Charakter einer Gruppe G. Dann ist für $g \in G$ $\chi(g)$ ganzalgebraisch über $\mathbb{Z}$.*

  Beweis. Es existiert eine Darstellung ρ, so dass $\chi = \mathrm{tr}(\rho)$ ist, d.h. $\chi(g)$ ist Summe der Eigenwerte von $\rho(g)$. Nun ist $\rho(g)$ von endlicher Ordnung, und damit seine Eigenwerte auch. Komplexe Zahlen endlicher Ordnung sind nichts anderes als Einheitswurzeln und damit wg. obiger Bemerkung ganzalgebraisch. $\chi(g)$ ist damit Summe ganzalgebraischer Zahlen (nämlich der Eigenwerte von $\rho(g)$) und somit ganzalgebraisch über $\mathbb{Z}$. □

  Damit wird auch klar, wo der Zusammenhang zwischen Ganzalgebraizität und der Charaktertheorie zu suchen ist.

- Es gibt auch einen Zusammenhang zwischen den Begriffen "ganz" und "ganzalgebraisch". Oberflächlich könnte man sagen, dass für Brüche p/q die Ganzalgebraizität daran scheitert, dass das Polynom in der Gleichung $qX - p = 0$ nicht normiert ist.

  Proposition 2.3. *Sei $p/q \in \mathbb{Q}$ eine über $\mathbb{Z}$ ganzalgebraische Zahl mit $q > 0$ und $\mathrm{ggT}(p, q) = 1$. Dann ist $q = 1$.*

  Beweis. $b := p/q$ ist Nullstelle eines normierten ganzzahligen Polynoms, etwa

  $$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0.$$

  Man kann dann folgendermaßen umformen:

  $$\begin{aligned} b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 &= 0 \\ p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p\, q^{n-1} + a_0 q^n &= 0 \\ q(a_{n-1}p^{n-1} + \cdots + a_1 p\, q^{n-2} + a_0 q^{n-1}) &= -p^n \end{aligned}$$

  Angenommen $q \neq 1$. Da die $a_i \in \mathbb{Z}$ vorausgesetzt waren, ist der Ausruck in der Klammer ganzzahlig. Also ist q ein Faktor in p^n, im Widerspruch dazu, dass p teilerfremd zu q vorausgesetzt war. □

  Wir wissen damit, dass $b \in \mathbb{Q}$ ganzalgebraisch über $\mathbb{Z}$ ist genau dann, wenn $b \in \mathbb{Z}$ ist. Man könnte sagen, dass $\mathbb{Z}$ in $\mathbb{Q}$ so etwas wie "ganz abgeschlossen" ist. Analog zeigt man, dass jeder faktorielle Ring in seinem Quotientenkörper ganz abgeschlossen ist.

Satz 2.4. *Seien $A \subset B$ eine Ringerweiterung und G die Menge der über A ganzalgebraischen Elemente. Dann ist G ein Ring, und es gilt $A \subset G \subset B$.*

Um dies zu zeigen, benötigen wir zwei Hilfsresultate.

Lemma 2.5. *Sei A ein Ring und $D = (d_{i,j}) \in A^{r \times r}$. Definiere dann die (so genannte zu D "adjunkte") Matrix*

$$D^* = (d^*_{ij}) = (-1)^{i+j}\det(D_{ji}),$$

wobei D_{ji} aus D durch Streichen der j-ten Zeile und i-ten Spalte hervorgeht. Man erhält

$$D\,D^* = D^*D = \det(D)I,$$

und insbesondere gilt für jeden Vektor $x \in A^r$

$$D\,x = 0 \Rightarrow \det(D)x = 0.$$

Beweis. (zu Lemma 2.5) Sei $E := D^*D = (e_{ij})$. Dann gilt

$$e_{ij} \;=\; \sum_{k=1}^{r} (-1)^{i+k} \det(D_{ki}) d_{kj}$$

Falls nun $i = j$ gilt, so ist nach dem Entwicklungssatz für Determinanten $e_{ii} = \det(D)$. Andernfalls kann man den Ausdruck als die Entwicklung einer Determinante auffassen, in der eine Spalte (die j-te, die ja in D_{ki} noch enthalten ist) doppelt vorkommt. Somit gilt für $i \neq j$ auch $e_{ij} = 0$. Für die zweite Behauptung mache man sich klar, dass

$$D\,x = 0 \Rightarrow D^*D\,x = 0 = \det(D)I\,x = \det(D)x = 0.$$

□

Nun wollen wir den Begriff der Ganzalgebraizität etwas abstrakter charakterisieren.

Lemma 2.6. *Sei* $A \subset B$ *eine Ringerweiterung. Dann gilt:* $b_1, ..., b_n \in B$ *sind ganzalgebraisch über* A *genau dann, wenn der Ring* $A[b_1, ..., b_n]$ *als* A*-Modul aufgefasst endlich erzeugt ist.*

Bemerkung 2.7. Seien $A \subset B \subset C$ Ringerweiterungen, und es sei B ein endlich erzeugter A-Modul und C ein endlich erzeugter B-Modul. Dann ist C auch ein endlich erzeugter A-Modul. (Man nimmt zwei Erzeugendensysteme $\{b_i\} \subset B, \{c_i\} \subset C$, dann ist $\{b_i c_j\}$ ein A-Erzeugendensystem von C.)

Beweis. (zu Lemma 2.6) " $\Rightarrow$ ": Wir betrachten zunächst den Fall $n = 1$. Sei $b \in B$ ganzalgebraisch über A, weiterhin $f \in A[X]$ das zu b gehörige normierte Polynom vom Grad $k \geqslant 1$. Sei $b' \in A[b]$. Dann lässt sich b' schreiben als $b' = g(b)$ mit einem Polynom $g \in A[X]$. Man kann dann eine Polynomdivision

$$g(x) = q(x)f(x) + r(x)$$

durchführen (der Leitkoeffizient von f ist schließlich eine Einheit), und es ergeben sich r, $q \in A[X]$ mit $\partial r < k$. Es gilt

$$g(b) = q(b)f(b) + r(b) = r(b) = a_0 + a_1 b + \cdots + a_{k-1} b^{k-1}.$$

D.h. unabhängig vom ursprünglichen Grad von g lässt sich b' bzgl. eines endlichen Erzeugendensystems $b^{k-1}, ..., b, 1$ darstellen.

Sei nun n beliebig. Wir zeigen die Behauptung durch Induktion nach n. Den Induktionsanfang ($n = 1$) haben wir gerade gezeigt. Sei die Behauptung nun gültig für $n - 1$, d.h. $R := A[b_1, ..., b_{n-1}]$ sei ein endlich erzeugter A-Modul. Dann ist b_n natürlich auch ganzalgebraisch über R, und somit ist $R[b]$ endlich erzeugter R-Modul. Wegen Bemerkung 2.7 wissen wir, dass auch $R[b]$ ein endlich erzeugter A-Modul ist.

" $\Leftarrow$ ": Sei der A-Modul $A[b_1, ..., b_n]$ endlich erzeugt, und $\omega_1, ..., \omega_r$ sei ein entsprechendes Erzeugendensystem. Dann kann für jedes Element $b \in A[b_1, ..., b_n]$ geschrieben werden

$$b\omega_i \;=\; \sum_{j=1}^{r} b_{ij}\omega_j$$

mit $b_{ij} \in A$. Setze nun $\omega := (\omega_1, ..., \omega_r)^T$ und $B := (b_{ij})$. Dann gilt

$$\begin{aligned} b\omega &= B\omega \\ \Rightarrow (b\,I - B)\omega &= 0 \\ (\text{Lemma 2.5}) \Rightarrow \det(b\,I - B)\omega &= 0 \\ \Rightarrow \det(b\,I - B)\omega_i &= 0. \end{aligned}$$

Da die ω_i ein Erzeugendensystem sind, lässt sich die 1 aus den ω_i linear kombinieren, etwa

$$1 = \sum_{i=1}^{r} \alpha_i \omega_i.$$

Setze $f(x) := \det(x\,I - B)$. Dann gilt

$$f(b) = \det(b\,I - B) = \sum_{i=1}^{r} \alpha_i \det(b\,I - B)\omega_i = 0,$$

und zusammen mit der Bemerkung, dass $f(x) \in A[X]$ ein normiertes Polynom ist, folgt die Behauptung. □

Beweis. (zu Satz 2.4) Hierzu ist im Wesentlichen zu zeigen, dass G bezüglich Multiplikation und Addition abgeschlossen ist. Seien dazu b_1, $b_2 \in G$. Betrachte nun den Ring $A[b_1, b_2]$, der offenbar bezüglich Multiplikation und Addition abgeschlossen ist. Setze $c := b_1 + b_2$, $d := b_1 b_2$. Dann ist $A[b_1, b_2, c] = A[b_1, b_2]$ als A-Modul noch immer endlich erzeugt, und daher sagt Lemma 2.6 angewandt auf $A[b_1, b_2, c]$, dass dann c auch ganzalgebraisch ist. Die gleiche Argumentation funktioniert auch für d. □

Bemerkung 2.8. Ein Element b ist ganzalgebraisch über $\mathbb{Z}$ genau dann, wenn sein Minimalpolynom in $\mathbb{Z}[X]$ liegt.

Beweis. Betrachte dazu die Nullstellen eines normierten Polynoms $g \in \mathbb{Z}[X]$. Alle Nullstellen von g sind ganzalgebraisch über $\mathbb{Z}$. Sei b eine solche Nullstelle. Hat b das Minimalpolynom f, so gilt $f \mid g$ in $\mathbb{Q}[X]$, d.h. f hat höchstens noch Koeffizienten in $\mathbb{Q}$. Nun sind aber die Nullstellen von f eine Untermenge derjenigen von g, und die waren alle ganzalgebraisch über $\mathbb{Z}$, also nach Proposition 2.3 schon in $\mathbb{Z}$. Durch Ausmultiplizieren erhält man, dass alle Koeffizienten von f in $\mathbb{Z}$ sind, was behauptet war. □

Mehr über ganzalgebraische Zahlen steht in [Neu92].

2.2 "Arithmetische Mittel" von Einheitswurzeln

Lemma 2.9. *Sei α die Summe von n Einheitswurzeln und weiter α/n ganzalgebraisch über $\mathbb{Z}$. Dann ist $\alpha/n = 0$ oder α/n ist selbst eine Einheitswurzel.*

Beweis. Sei f das Minimalpolynom zu α/n über $\mathbb{Z}$. f habe über seinem Zerfällungskörper K die Nullstellen $\beta_1, ..., \beta_k$, d.h.

$$f(x) = \prod_{i=1}^{k} (x - \beta_i).$$

$f \in \mathbb{Z}[X]$ ist normiert und seine Koeffizienten ganzzahlig (Bemerkung 2.8), d.h. insbesondere gilt also für den Koeffizienten 0-ter Ordnung

$$c := \prod_{i=1}^{k} \beta_i \in \mathbb{Z}.$$

Jedes dieser β_i kann wie α als ein "arithmetisches Mittel" von Einheitswurzeln geschrieben werden: $K/\mathbb{Q}$ ist galoissch (weil normal und separabel), und es gilt $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, ..., \sigma_k\}$ mit (o.B.d.A.) $\sigma_i(\alpha/n) = \beta_i$. Nehmen wir nun an, es sei $\alpha = \theta_1 + \cdots + \theta_n$, wobei die θ_i die o.g. Einheitswurzeln seien. Gelte also $\theta_j^m = 1$. Dann ergibt sich $\sigma_i(\theta_j)^m = \sigma_i(\theta_j^m) = \sigma_i(1) = 1$, also ist auch $\sigma_i(\theta_j)$ eine Einheitswurzel für alle $i = 1, ..., k$, $j = 1, ..., n$. Leicht macht man sich klar, dass weiter $\sigma_i(n) = \sigma_i(1 + 1 + \cdots + 1) = n$ ist, so dass jedes

$$\beta_i = \sigma_i(\alpha/n) = \sigma_i((\theta_1 + \cdots + \theta_n)/n) = (\sigma_i(\theta_1) + \cdots + \sigma_i(\theta_k))/n$$

tatsächlich in der verlangten Form geschrieben werden kann.

Daher gilt $|\beta_i| \leqslant 1$ für $i = 1, ...k$, und somit $c \in \{-1, 0, 1\}$. Ist nun irgendein $|\beta_i| < 1$, so gilt $|c| < 1$, insofern $c = 0$. Damit ist eines der β_i schon gleich Null gewesen. Nun sind die β_i zueinander konjugiert, d.h. sie sind alle Null, somit auch α/n.

Ansonsten muss $|\alpha/n| = 1$, also $|\alpha| = n$ sein. Mit der Dreiecksungleichung gilt ohnehin

$$|\alpha| = |\theta_1 + \theta_2 + \cdots + \theta_n| \leqslant n,$$

Gleichheit tritt hier lediglich bei paarweise linearer Abhängigkeit ein (wie in der Cauchy-Schwarzschen Ungleichung, die zum Beweis der Dreiecksungleichung verwendet werden kann). Somit sind die θ_i linear abhängig, also gleich. Daher gilt nun $\alpha = n\theta$. □

2.3 Charaktertheoretische Vorbereitungen

Erinnern wir uns an das Folgende, das in [Kra03] und [Noa03] definiert und bewiesen wurde:

Definition 2.10. *Sei G eine endliche Gruppe und $\chi_1, \chi_2 : G \to \mathbb{C}$ Funktionen. Dann sei*

$$(\chi_1|\chi_2) := \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)}.$$

$(\chi_1|\chi_2)$ ist ein Skalarprodukt.

Satz 2.11. *Seien χ_k für $k = 1, ..., r$ die irreduziblen Charaktere einer endlichen Gruppe G. Es gilt dann für $i, j \in \{1, ..., r\}$*

$$(\chi_i|\chi_j) = \delta_{ij}.$$

Die Charaktere χ_k bilden eine Orthogonalbasis im Vektorraum der Klassenfunktionen.

In [Noa03] haben wir gesehen, dass es gleich viele irreduzible Darstellungen einer Gruppe G wie Konjugiertenklassen in G gibt. Wir erhalten ein Resultat, das man analog zur obigen "ersten" vielleicht die "zweite Orthogonalitätsrelation" nennen könnte.

Satz 2.12. *Seien χ_k für $k = 1, ..., r$ die irreduziblen Charaktere einer endlichen Gruppe G. Weiter seien g_k für $k = 1, ..., r$ Vertreter der k-ten Konjugationsklasse C_k in G und c_k die Anzahl $|C_k|$ der Elemente in dieser Konjugationsklasse. Dann gilt*

$$\sum_{k=1}^{r} \chi_k(g_i)\overline{\chi_k(g_j)} = \delta_{ij}\frac{|G|}{c_i}.$$

Beweis. Sei nun f_j die charakteristische Funktion von C_j. Dann lässt sich f_j leicht aus Charakteren linear kombinieren:

$$\delta_{ij} = f_j(g_i) = \sum_{k=1}^{r} (f_j|\chi_k)\chi_k(g_i), \qquad \text{wobei } (f_j|\chi_k) = \frac{c_j}{|G|}\overline{\chi_k(g_j)}.$$

Zusammenfassend erhalten wir

$$\delta_{ij} = \sum_{k=1}^{r} \frac{c_j}{|G|}\chi_k(g_i)\overline{\chi_k(g_j)}$$

und somit

$$\sum_{k=1}^{r} \chi_k(g_i)\overline{\chi_k(g_j)} = \delta_{ij}\frac{|G|}{c_j}.$$

Wenn man sich überlegt, dass die rechte Seite ohnehin Null ist, wenn $i \neq j$, dann kann man statt c_j sicher auch c_i schreiben. □

Satz 2.13. *Mit der Notation aus Satz 2.12 gilt, dass*

$$c_j\frac{\chi_i(g_j)}{\chi_i(1)}$$

eine ganzalgebraische Zahl über $\mathbb{Z}$ ist.

Beweis. Sei $n_k := \chi_k(1)$ und ρ_k eine zu χ_k gehörige Darstellung ($k \in \{1, ..., r\}$), mit der wir setzen

$$\Phi := \sum_{x \in C_j} \rho_i(x) \in \mathrm{End}(\mathbb{C}^{n_i}) = \mathbb{C}^{n_i \times n_i}.$$

Für jedes $g \in G$ gilt dann

$$\begin{aligned} \rho_i(g)\Phi\rho_i(g)^{-1} &= \rho_i(g)\left(\sum_{x \in C_j} \rho_i(x)\right)\rho_i(g)^{-1} \\ &= \sum_{x \in C_j} \rho_i(g\,x\,g^{-1}) \\ &= \sum_{x \in C_j} \rho_i(x) = \Phi. \end{aligned}$$

Dann ist $\Phi = \omega_{ij} I_{n_i}$ nach dem Lemma von Schur. Nun gilt

$$n_i\omega_{ij} = \mathrm{tr}(\Phi) = \sum_{x \in C_j} \mathrm{tr}(\rho_i(x)) = \sum_{x \in C_j} \chi_i(x) = c_j\chi_i(g_j),$$

oder äquivalent

$$\omega_{ij} = c_j \frac{\chi_i(g_j)}{n_i}.$$

Offenbar genügt es damit an dieser Stelle zu zeigen, dass die ω_{ij} ganzalgebraisch sind.

Sei σ die reguläre Darstellung mit Darstellungsraum V und

$$\Psi := \sum_{x \in C_j} \sigma(x).$$

Wie bei früher gesehen zerfällt

$$\sigma = \bigoplus_{k=1}^{r} m_k\rho_k \qquad \text{und} \qquad V = \bigoplus_{k=1}^{r} m_k V_k,$$

wobei die V_k die Darstellungsräume der ρ_k seien. O.E. nehmen wir $m_k = 1$ an für $k = 1, ...r$. Für ein $v \in V_i \setminus \{0\}$ gilt wie oben gezeigt $\Phi(v) = \omega_{ij}v$. Wir können nun v als Element von V auffassen und schreiben

$$v = \bigoplus_{k=1}^{r} v_k,$$

wobei natürlich alle v_k bis auf v_i Null sind. Wir erhalten

$$\begin{aligned} \Psi(v) &= \sum_{x \in C_j} \sigma(x)(v) = \sum_{x \in C_j} \bigoplus_{k=1}^{r} \rho_k(v_k) \\ &= \sum_{x \in C_j} \rho_i(v_i) = \Phi(v) = \omega_{ij}v. \end{aligned}$$

Also ist ω_{ij} auch Eigenwert von Ψ.

Der Darstellungsraum der regulären Darstellung kann geschrieben werden als ein Vektorraum, der von Basiselementen $(e_g)_{g \in G}$ aufgespannt wird. Untersuchen wir nun die Wirkung von Ψ auf diese Basis von V:

$$\begin{aligned} \Psi(e_g) &= \sum_{h' \in C_j} \sigma(h')(e_g) = \sum_{h' \in C_j} e_{h'g} \\ &= \sum_{h' \in G} \mathbf{1}\{h' \in C_j\} e_{h'g} \\ (\text{setze } h := h'g \to h' = h\,g^{-1}) &= \sum_{hg^{-1} \in G} \mathbf{1}\{h\,g^{-1} \in C_j\} e_h \\ &= \sum_{h \in G} \mathbf{1}\{h\,g^{-1} \in C_j\} e_h. \end{aligned}$$

Setzen wir $a_{gh} := \mathbf{1}\{h\,g^{-1} \in C_j\}$, so erhalten wir eine Darstellungsmatrix von Ψ, die ausschließlich aus ganzzahligen Einträgen besteht, d.h. deren charakteristisches Polynom ganzzahlig und normiert ist. ω_{ij} ist Eigenwert dieser Matrix, Nullstelle dieses charakteristischen Polynoms und somit ganzalgebraisch. □

3 Burnsides p^aq^b-Satz

In diesem Kapitel verwenden wir weiterhin die Notation von Satz 2.12.

Lemma 3.1. *Seien $\chi_i(1)$ und c_j für $i, j \in \{1, ..., r\}$ teilerfremd. Dann ist $\chi_i(g_j)/\chi_i(1) = 0$ oder $\chi_i(g_j)/\chi_i(1)$ ist eine Einheitswurzel.*

Beweis. Der $\mathrm{ggT}(\chi_i(1), c_j) = 1$, d.h. es existieren zwei ganze Zahlen $a, b \in \mathbb{Z}$, so dass

$$a\chi_i(1) + b\,c_j = 1.$$

Wenn wir mit $\chi_i(g_j)/\chi_i(1)$ durchmultiplizieren, erhalten wir

$$a\chi_i(g_j) + b\,c_j\,\frac{\chi_i(g_j)}{\chi_i(1)} = \frac{\chi_i(g_j)}{\chi_i(1)}.$$

Wegen Satz 2.13 ist nun der zweite Term eine ganzalgebraische Zahl. Der erste Term ist eine ganzalgebraische Zahl wegen Folgerung 2.2. Aufgrund der Abgeschlossenheit der ganzalgebraischen Zahlen muss damit auch $\chi_i(g_j)/\chi_i(1)$ ganzalgebraisch sein. $\chi_i(1)$ ist eine natürliche Zahl und $\chi_i(g_j)$ eine Summe von $\chi_i(1)$ Einheitswurzeln. Mit Lemma 2.9 folgt daher die Behauptung. □

Definition 3.2. *Eine Gruppe G heißt einfach genau dann, wenn sie als Normateiler nur $\{1\}$ und sich selbst hat.*

Lemma 3.3. *Sei $g_i \in G$, und es gelte $c_i = p^a$, wobei p eine Primzahl und $a \geqslant 1$ eine ganze Zahl sind. Dann ist G nicht einfach.*

Bemerkung 3.4. Sei ρ: $G \to \mathrm{GL}(n, \mathbb{C})$ Darstellung von G. Dann ist $\rho(G)$ ebenfalls eine Gruppe.

Bemerkung 3.5. Sei $\rho: G \to \mathrm{GL}(n, \mathbb{C})$ Darstellung von G und $N \trianglelefteq \rho(G)$. Dann ist $\rho^{-1}(N) \trianglelefteq G$.

Beweis. (zu Lemma 3.3) Nach Satz 2.12, angewendet auf das Gruppenelement g_i und das neutrale Element $g_j := 1 \in G$, gilt

$$\sum_{k=1}^{r} \chi_k(g_i)\overline{\chi_k(g_j)} = \delta_{ij}\frac{|G|}{c_i} = 0,$$

denn die Konjugiertenklasse der 1 umfasst auch nur diese, d.h. $g_i \sim 1$ kann nicht auftreten. Unter der Annahme, dass $\chi_1 = 1$ der triviale Charakter ist, kann man dies umformen zu

$$\begin{aligned} 0 &= \sum_{k=1}^{r} \chi_k(g_i)\overline{\chi_k(1)} = \sum_{k=1}^{r} \chi_k(g_i)\chi_k(1^{-1}) \\ &= \sum_{k=1}^{r} \chi_k(g_i)\chi_k(1) \\ &= 1 + \sum_{k=2}^{r} \chi_k(g_i)\chi_k(1). \end{aligned}$$

Wir wollen zeigen, dass in der Summe oben ein Summand vorkommt, in dem $p \nmid \chi_k(1)$ und $\chi_k(g_i) \neq 0$. Nehmen wir einmal an, für $p \nmid \chi_k(1)$, wäre automatisch $\chi_k(g_i) = 0$. Dann wäre $\chi_k(1)/p$ für alle verbliebenen k ganzzahlig und man könnte schreiben

$$\begin{aligned} 0 &= 1 + p\,m \\ \text{mit } m &= \sum_{k=2,\,\chi_k(g_i)\neq 0}^{r} \chi_k(g_i)\frac{\chi_k(1)}{p}. \end{aligned}$$

Dann wäre $m = -1/p$. Durch Folgerung 2.2 wissen wir, dass m als Summe über $\mathbb{Z}$ ganzalgebraischer Elemente selbst ganzalgebraisch über $\mathbb{Z}$ ist. Das ist $-1/p$ aber nicht (vgl. Proposition 2.3). Damit war unsere Annahme falsch.

Somit existiert zumindest ein k mit $\chi_k(g_i) \neq 0$ und $p \nmid \chi_k(1)$. Es sind also $\chi_k(1)$ und p teilerfremd, damit auch $\chi_k(1)$ und $p^a = c_i$. Da wir $\chi_k(g_i) \neq 0$ vorausgesetzt hatten, ist $\chi_k(g_i) = \lambda\chi_k(1)$ mit einer Einheitswurzel λ nach Lemma 3.1. Sei dann $\rho_k = \lambda I$ die zu χ_k gehörige Darstellung. Dann ist $\rho_k(g) \in Z(\rho_k(G))$ (beachte Bemerkung 3.4). Dies bedeutet, dass $\rho_k(G)$ einen nichttrivialen Normalteiler hat, denn das Zentrum ist ja einer, und andererseits war χ_k ein nichttrivaler Charakter, wodurch ρ_k auch nicht die triviale Darstellung sein kann. Nach Bemerkung 3.5 ist dann

$$\rho_k^{-1}(Z(\rho_k(G))) \trianglelefteq G$$

und da $Z(\rho_k(G))$ schon ein nichttriviales Element enthielt, muss sein Urbild dies auch tun. Also ist $Z(G)$ nichttrivial. Da aber wegen $c_i = p^a$ eine echte Konjugationsklasse in G existiert, gilt auch $Z(G) \neq G$. Daher ist G nicht einfach. □

Lemma 3.6. *(Burnside) Seien p, q Primzahlen, $a, b \in \mathbb{N} \cup \{0\}$, $p \neq q$. Sei G eine Gruppe mit $\mathrm{ord}(G) = p^a q^b$ für $a, b \geqslant 1$. Dann ist diese Gruppe nicht einfach.*

Bemerkung 3.7. Sei p prim und G eine p-Gruppe der Ordnung p^k mit $k \geqslant 1$. Dann hat G ein nichttriviales Zentrum.

Beweis. (zu Bemerkung 3.7) Die Klassengleichung für die Konjugationsoperation von G auf sich besagt

$$\mathrm{ord}(G) = \mathrm{ord}(Z(G)) + \sum_{i=1}^{n} (G : Z_{\{x_i\}}),$$

wobei $x_1, ..., x_n$ ein Vertretersystem der G-Bahnen in $G \setminus Z$ ist. Die Ausdrücke $\mathrm{ord}(G)$ und $(G : Z_{\{x_i\}})$ sind echte p-Potenzen ($Z_{\{x_i\}}$ ist echte Untergruppe von G wegen $x_i \notin Z(G)$), also auch $\mathrm{ord}(Z(G))$. Wegen $1 \in Z(G)$ ist das Zentrum nichttrivial. □

Bemerkung 3.8. Ist p eine Primzahl, G eine endliche Gruppe und gilt $p|\mathrm{ord}(G)$, so hat G ein Element der Ordnung p. (5.2.11 in [Bos99])

Beweis. (zu Lemma 3.6) Sei S eine p-Sylowgruppe in G. Wegen Bemerkung 3.7 existiert ein $z \in Z(S) \setminus \{1\}$. Die Konjugationsklasse von z (Bahn von z unter der Konjugationsoperation) hat dann $n := \mathrm{ord}(G)/\mathrm{ord}(Z_G(z))$ Elemente, da die Anzahl der Elemente in einer Bahn ja gerade der Index der Isotropiegruppe ist. Betrachte

$$Z_G(z) = \{g \in G \,|\, g\,z = z\,g\}.$$

Nach Festlegung kommutiert z mit sämtlichen Elementen von S, d.h. $S \subset Z_G(z)$. S war p-Sylowgruppe, d.h. $\mathrm{ord}(S) = p^a$. Also kann n höchstens noch eine q-Potenz sein. Ist n eine echte q-Potenz, so erhalten wir mit Lemma 3.3, dass G nicht einfach ist. Ist $n = 1$, so gilt $z \in Z(G)$, denn dann gilt $Z_G(z) = G$, d.h. z vertauscht mit ganz G. Dann hat aber G ein nichttriviales Zentrum, und es gibt nach Bemerkung 3.8 ein Element h von Primzahlordnung in $Z(G)$. Dann ist $\langle h \rangle \lhd G$ (und auch $\langle h \rangle \neq G$) und damit G nicht einfach. □

Mit diesen Sätzen sind wir nun endlich in der Lage, ein recht informatives Resultat über Gruppen der Ordnung $p^a q^b$ zu zeigen. Erinnern wir uns:

Definition 3.9. *Sei G eine endliche Gruppe. Eine Kette von Untergruppen*

$$\{1\} \lhd G_n \lhd ... \lhd G_1 \lhd G_0 = G$$

heißt eine Normalreihe von G. Die zur Kette gehörigen Restklassengruppen G_i/G_{i+1} werden als Faktoren der Normalereihe bezeichnet. ($i = 0, ..., n-1$). G heißt auflösbar, wenn G eine Normalreihe mit zyklischen Faktoren von Primpotenzordnung besitzt. (Anmerkung: In [Bos99] wird für Auflösbarkeit lediglich Kommutativität verlangt)

Satz 3.10. *(Burnside) Seien p, q Primzahlen, $a, b \in \mathbb{N} \cup \{0\}$, $p \neq q$. Sei G eine Gruppe mit $\mathrm{ord}(G) = p^a q^b$. Dann ist diese Gruppe auflösbar.*

Beweis. Wir benutzen vollständige Induktion nach $a+b$. Für $a=0$ oder $b=0$ ist die Behauptung klar, p-Gruppen sind schließlich auflösbar. Sei also $a,b \geqslant 1$ und sei G eine Gruppe der Ordnung $p^a q^b$.

Lemma 3.6 verrät uns, dass G einen einen Normalteiler N hat, der nicht die ganze Gruppe ist, aber auch nicht $\{1\}$. Habe N die Ordnung $p^{a_1}q^{b_1}$ und G/N die Ordnung $p^{a_2}q^{b_2}$. Dann sind sicher $a_1+b_1 < a+b$ und $a_2+b_2 < a+b$. Nach Induktionsvoraussetzung sind also beide auflösbar, und wir erhalten Ketten von Untergruppen der Form

$$\begin{aligned} \{1\} &= G_0 \lhd G_1 \lhd \cdots \lhd G_s = N \\ \{1\} &= G_s/N \lhd G_{s+1}/N \lhd \cdots \lhd G_r/N = G/N \end{aligned}$$

mit definitionsgemäßen Faktoren. Die großen Gruppen $G_{s+1}, ..., G_r$ erhält man dabei als Urbild der Faktorgruppen unter der kanonischen Projektion. Dann zeigt die Kette

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$$

die Auflösbarkeit von G. □

4 Schlussbemerkungen

Abschließend kann man beobachten, dass sich unser Resultat mit altbekannten Dingen deckt: Die S_4 hat als Ordnung $2 \cdot 3 \cdot 4 = 2^3 \cdot 3$, ist also von der hier behandelten p^aq^b-Form. Und sie ist auflösbar, der Satz stimmt also. Die S_5 enthält mit $2 \cdot 3 \cdot 4 \cdot 5 = 2^3 \cdot 3 \cdot 5$ bereits drei Primzahlen – und ist nicht auflösbar. Damit ist klar, dass wir in gewisser Hinsicht "die Grenze" erreicht haben: Ein analoger Satz für Produkte dreier Primzahlpotenzen kann nicht gelten.

Als abschließender Schulterklopfer für dieses Seminar bleibt zu sagen, dass bislang laut [Col90] kein Beweis für diesen Satz ohne Charaktertheorie ausgekommen ist.

Literaturverzeichnis

[Bos99] Siegfried Bosch. *Algebra*. Springer, 1999.

[Col90] Michael J. Collins. *Representations and characters of finite groups*. Cambridge University Press, Cambridge, 1990.

[JL93] Gordon James and Martin Liebeck. *Representations and Characters of Groups*. Cambridge University Press, 1993.

[Kra03] Mirko Kraft. Charaktere 1. Vortrag im Seminar Darstellungstheorie, S. Kühnlein, C.-G. Schmidt, 2003.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer, 1992.

[Noa03] Benjamin Noack. Charaktere 2. Vortrag im Seminar Darstellungstheorie, S. Kühnlein, C.-G. Schmidt, 2003.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*. Springer, 1977.