Anwendung von Burnside-Ringen auf endliche Gruppen

Till Müller

13. November 2023

Diese Ausarbeitung unterteilt sich in zwei Kapitel. Zunächst wird in Kapitel 1 der Burnside-Ring $\Omega(G)$ einer endlichen Gruppe G definiert und die Elemente in $\Omega(G)$ charakterisiert. Für eine Untergruppe $U \leq G$ operiert jede Untergruppe $K \leq G$ auf der G-Menge G/U durch Linksmultiplikation. Die Anzahl der Fixpunkte von G/U unter K wird als Abbildung $\varphi_K(G/U)$ beschrieben. Mithilfe dieser Abbildung und der Existenz des Wieland-Frobenius Homomorphismus Satz 2.2 lassen sich einige Aussagen der elementaren endlichen Gruppentheorie folgern. Dies werden wir in Kapitel 2 untersuchen. Unter anderem werden wir die Sätze von Sylow sowie Kongruenzen von Frobenius zeigen. Dabei richten wir uns im ersten Kapitel nach [Die79] und ab Bemerkung 1.13, sowie in dem zweiten Kapitel, nach [DSY92].

Stets sei G eine endliche Gruppe.

1 Grundlagen

Definition 1.1 (i) Eine endliche Menge M heißt *G-Menge*, falls G auf M operiert durch Linksmultiplikation. D.H. es existiert eine Abbildung $G \times M \to M, (g, m) \mapsto gm$ sodass $(g_1 g_2)m = g_1(g_2 m)$ und $1m = m$ für alle $g_1, g_2 \in G, m \in M$.

(ii) Wenn M, N G-Mengen sind, so heißt $\psi \colon M \to N$ *G-Abbildung*, falls $\psi(gm) = g\psi(m)$ für alle $g \in G, m \in M$.

(iii) Zwei G-Mengen M, N heißen *G-isomorph* oder auch *isomorph als G-Mengen*, falls eine bijektive G-Abbildung zwichen M und N existiert. Ggf. schreiben wir $M \cong_G N$. Die G-Isomorphieklasse von M bezeichnen wir mit $[M]$ und die Menge aller G-Isomorphieklassen als $\tilde{G}$.

Wir können stets annehmen, dass zwei M, N G-Mengen disjunkt sind. Die disjunkte Vereinigung $M \sqcup N$ und das kartesische Produkt $M \times N$ sind ebenfalls G-Mengen auf natürliche Weise, d.h von M und N wird auf $M \sqcup N$ die Operation von G fortgesetzt und für $n \in N, m \in M, g \in G : g(m, n) \coloneqq (gm, gn)$.

Definition 1.2 Für G-Mengen M, N definieren wir $[M] + [N] \coloneqq [M] \sqcup [N]$, $[M] \cdot [N] \coloneqq [M] \times [N]$ und erhalten mit $0 = [\emptyset], 1 = [\{1\}]$ einen kommutativen Halbring der Isomorphieklassen von G-Mengen.

Um einen Ring aus den G-Isomorphieklassen zu erhalten benötigen wir noch das additive Inverse. Wie üblich definieren wir uns eine geeignete Äquivalenzrelation und erhalten einen Ring auf der Quotientenmenge.

Definition 1.3 Auf $\tilde{G} \times \tilde{G}$ definieren wir die Äquivalenzrelation

$$([M_1], [M_2]) \sim ([N_1], [N_2]) : \iff [M_1] + [N_2] = [M_2] + [N_1].$$

Die Äquivalenzklasse von $([M], [N])$ bezeichnen wir als $[M]-[N]$. Auf $\Omega(G) \coloneqq (\tilde{G} \times \tilde{G})/\sim$ definieren wir die Addition und Multiplikation durch

$$\begin{aligned}([M_1] - [M_2]) + ([N_1] - [N_2]) &\coloneqq ([M_1] + [N_1]) - ([M_2] + [N_2]),\\ ([M_1] - [M_2]) \cdot ([N_1] - [N_2]) &\coloneqq ([M_1] \cdot [N_1] + [M_2] \cdot [N_2]) - ([M_1] \cdot [N_2] + [M_2] \cdot [N_1]).\end{aligned}$$

Mit $0 = ([\emptyset], [\emptyset]), 1 = ([\{1\}], [\emptyset])$ wird $\Omega(G)$ zu einem Ring, den wir als *Burnside-Ring von G* bezeichnen. Wir werden für eine G-Menge $M \neq \emptyset$ die Restklassen $([M], [\emptyset])$ und $([\emptyset], [M])$ mit $[M]$ und $-[M]$ bezeichnen.

Wir möchten die Elemente von $\Omega(G)$ charakterisieren. Hierfür werden wir zunächst die Darstelllung von transitiven G-Mengen herleiten, um auf die Äquivalenzklassen von beliebigen G-Mengen zu schließen.

Lemma 1.4 *Sei M eine transitive G-Menge, $m \in M$ und G_m der Stabilisator von m. Dann definiert $\psi\colon G/G_m \to M, gG_m \mapsto gm$ einen G-Isomorphismus. Insbesondere gilt $|M| \mid |G|$.*

Beweis: Wohldefiniertheit und Injektivität:

$$gG_m = hG_m \iff g^{-1}h \in G_m \iff g^{-1}hm = m \iff hm = gm.$$

Die Surjektivität folgt durch die Transitivität. Nun gilt $\psi(ghG_m) = ghm = g\psi(hG_m)$. Folglich ist ψ ist ein G-Isomorphismus und $G/G_m \cong_G M$. Die Letzte Aussage folgt direkt mit dem Satz von Lagrange und der Gleichheit $|M| = |G/G_m|$. □

Bemerkung 1.5 Sei $U \leq G$. Dann sind die Nebenklassen G/U eine transitive G-Menge, d.h die Operation von G auf G/U ist definiert durch Linksmultiplikation. Außerdem existiert nach Lemma 1.4 für jede transitive G-Menge M eine Untergruppe $U \leq G$ mit $M \cong_G G/U$. Folglich hat jede transitive G-Isomorphieklasse die Form $[G/U]$.

Seien $U, K \leq G$. Dann gilt bekanntlich

$$G/U \cong_G G/K \iff \exists g \in G : g^{-1}Ug = K.$$

Insbesondere ist $G/U \ncong_G G/K$, sofern $U \cong K$ aber nicht konjugiert sind. Aus Isomorphie von Unterruppen, erhalten wir daher nicht unbedingt G-Isomorphie der entsprechenden Nebenklassen. Außerdem besteht die G-Isomorphieklasse $[G/U]$ aus allen Nebenklassen von Untergruppen die zu U konjugiert sind in G.

Bemerkung 1.6 Jede G-Menge M gleicht ihrer eindeutigen disjunkten Vereinigung der Bahnen von G auf M. Seien $w_1, \ldots, w_r$ die Bahnen auf M. So erhalten wir $M = \sqcup_{i=1}^{r} w_i$. Nun ist jede Bahn bereits transitiv. Nach Lemma 1.4 existieren eindeutige Untergruppen (bis auf Konjugation) $U_i \leq G$ mit $i = 1, \ldots, r$, sodass

$$M = \sqcup_{i=1}^{r} w_i = \sqcup_{i=1}^{r} G/U_i$$

gilt. Somit gilt bis auf G-Isomorphie

$$[M] = [\sqcup_{i=1}^{r} G/U_1] = \sum_{i=1}^{r} [G/U_i].$$

Von nun an werden wir G/U anstelle von $[G/U]$ schreiben.

Lemma 1.7 *Jedes $x \in \Omega(G)$ lässt sich darstellen durch*

$$x = \sum_{U \leq G}{}' \mu_U(x) \cdot G/U,$$

für eindeutig bestimmte $\mu_U(x) \in \mathbb{Z}$. Dabei bezeichnet das Summationssymbol $\sum'$, dass die Summe lediglich über die Repräsentaten von Konjugationsklassen von Untergruppen summiert. Insbesondere gilt $\mu_U(x) = \mu_{gUg^{-1}}(x)$ für alle $g \in G$.

Beweis: Die Aussage folgt direkt aus Bemerkung 1.6. □

Bemerkung 1.8 Seien $U, K \leq G$. Um das Produkt $G/U \cdot G/K \in \Omega(G)$ zu klassifizieren, muss man die Bahnen bzw. Stabilisatoren berechnen. Der Stabilisator von einem Element $(g_1U, g_2K) \in G/U \cdot G/K$ ist gegeben durch

$$\begin{aligned} G_{(g_1U, g_2K)} &= \{g \in G : (gg_1U, gg_2K) = (g_1U, g_2K)\} \\ &= G_{g_1U} \cap G_{g_2K} \\ &= g_1 U g_1^{-1} \cap g_2 K g_2^{-1}. \end{aligned}$$

Sei G eine abelsche Gruppe. Damit folgt $G_{(g_1U, g_2K)} = U \cap K$. Daher sind die Stabilisatoren von allen Elementen identisch, d.h alle Bahnen sind identisch. Wir erhalten $G/U \cdot G/K = a \cdot G/(U \cap K)$ mit $a = \frac{|G| \cdot |U \cap K|}{|U| \cdot |K|} = \frac{|G|}{|UK|}$, das bedeutet a erhält man durch abzählen der Elemente auf beiden Seiten. Für $K = U$ erhält man $(G/U)^2 = |G : U| \cdot G/U$.

Beispiel 1.9 Sei $G = S_3$, $U = <(1,2)> \leq G$ und $M \coloneqq G/U = \{U, (1,2,3)U, (1,3,2)U\}$. Wir möchten M^2 berechnen und nutzen hierfür Bemerkung 1.8. Es gilt

$$\begin{aligned} <(1,2)> &= U, & U &= (1,2)U(1,2), \\ <(1,3)> &= (1,2,3)U(1,3,2), & <(1,3)> &= (2,3)U(2,3), \\ <(2,3)> &= (1,3,2)U(1,2,3), & <(2,3)> &= (1,3)U(1,3). \end{aligned}$$

Nun gilt bereits $G_{(xU,yU)} = xUx^{-1} \cap yUy^{-1}$ für $(xU, yU) \in M^2$. Die einzigen Paare $(x,y) \in G^2$ für die $xUx^{-1} \cap yUy^{-1} \neq 1$ gilt, sind gegeben durch $((2,3),(1,2,3))$, $((1,3),(1,3,2))$, $(1,(1,2))$. Allerdings sind $(1,2),(2,3),(1,3)$ konjugiert zueinander. Daher sind die G-Mengen G/V mit $V \in \{<(1,3)>, <(2,3)>, <(1,2)>\}$ in der gleichen G-Isomorphieklasse. Da die Stabilisatoren dieser Paare alle gleich sind und die Bahnen jeweils drei Elemente enthalten, sind alle drei Paare in der gleichen Bahn. Für die restlichen 6 Paare gilt $G_{(xU,yU)} = 1$. Folglich sind die jeweiligen Bahnen G-isomorph zu $G/1$, welche ebenfalls 6 Elemente besitzt. Wir erhalten $M^2 = G/U + G/1$.

Sei $H \leq G$, M, N G-Mengen, dann operiert H auf den Mengen M, N. Wir definieren

$$M^H \coloneqq \mathrm{fix}_H(M) \coloneqq \{m \in M : hm = m \ \forall h \in H\}.$$

Lemma 1.10 *Sei $H \leq G$, M, N G-Mengen und $g \in G$. Dann gilt $|M^H + N^H| = |M^H| + |N^H|$, $|(M \times N)^H| = |M^H| \cdot |N^H|$ und $|M^{g^{-1}Hg}| = |M^H|$.*

Beweis: Es gilt

$$\begin{aligned} |M^H + N^H| &= |M^H \sqcup N^H| \\ &= |\{x \in M \sqcup N : hx = x \ \forall h \in H\}| \\ &= |\mathrm{fix}_H(M)| + |\mathrm{fix}_H(N)| = |M^H| + |N^H| \end{aligned}$$

und

$$\begin{aligned} |(M \times N)^H| &= |\{(m,n) \in M \times N : h(m,n) = (hm, hn) \ \forall h \in H\}| \\ &= |M^H| \cdot |N^H|. \end{aligned}$$

Sei $U \leq G$, so ist

$$\begin{aligned} |(G/U)^{g^{-1}Hg}| &= |\{g'U \in G/U : xg'U = g'U \ \forall x \in g^{-1}Hg\}| \\ &= |\{g'U \in G/U : h(gg'U) = (gg'U) \ \forall h \in H\}| \\ &= |\{g'U \in G/U : hg'U = g'U \ \forall h \in H\}| \\ &= |(G/U)^H|. \end{aligned}$$

Folglich gilt mit $M \cong \sqcup_{i=1}^n G/U_i$, d.h U_i sind nicht konjugiert zueinander,

$$\begin{aligned} |M^{g^{-1}Hg}| &= |\sqcup_{i=1}^n (G/U_i)^{g^{-1}Hg}| \\ &= \prod_{i=1}^n |(G/U_i)^H| = |M^H|. \end{aligned}$$

□

Bemerkung 1.11 Nach Lemma 1.10 ist die Abbildung

$$\varphi_H \colon \Omega(G) \to \mathbb{Z},$$
$$\sum_{U \leq G}{}' \mu_U(x) G/U \mapsto \sum_{U \leq G}{}' \mu_U(x) \cdot |(G/U)^H|$$

für $H \leq G$ wohldefiniert und sogar ein Ring Homomorphismus. Insbesondere ist $\varphi_U = \varphi_H$ für alle zu H konjugierten Untegruppen $U \leq G$. Sei $C(G)$ die Menge der Konjugationsklassen der Untergruppen von G. So definieren wir das Produkt der φ_H als

$$\varphi = (\varphi_H) \colon \Omega(G) \to \bigtimes_{H \in C(G)} \mathbb{Z}.$$

Lemma 1.12 *Die Abbildung φ ist ein injektiver Ring Homomorphismus.*

Beweis: Angenommen $x \neq 0 \in \Omega(G)$ sei im Kern von φ. Um dies in einen Widerspruch zu führen finden wir eine Untergruppe $H \leq G$ mit $\varphi_H(x) \neq 0$. Offenbar erhalten wir eine Halbordnung (Reflexiv, Antisymmetrisch und Transitiv) auf $\{G/U : U \leq G\}$ durch $G/H \leq G/U$ genau dann, wenn H eine Untergruppe zu einer zu U konjugierten Untergruppe ist. Sei G/U maximal in bezug auf die oben beschriebene Ordnung mit $\mu_U(x) \neq 0$. Nehmen wir an $(G/K)^U \neq \emptyset$ für $K \leq G$. Damit folgt $\exists gK \in G/K$ mit $ugK = gK \ \forall U$. Folglich gilt $g^{-1}UgK = K$, d.h $U \subset gKg^{-1}$. Demnach gilt $G/U \leq G/K$. Nun ist G/U maximal gewählt mit $\mu_U(x) \neq 0$, folglich ist $\mu_K(x) = 0$ oder K kunjugiert zu U. Somit ist

$$\begin{aligned} 0 = \varphi_U(x) = \mu_U(x)|(G/U)^U| &= \mu_U(x)|\{gU \in G/U : g^{-1}UgU = U\}| \\ &= \mu_U(x)|\{gU \in G/U : g \in N_G(U)\}| \\ &= \mu_U(x)|N_G(U) : U| \neq 0. \end{aligned}$$

Dies ist ein Widerspruch. □

Insbesondere gilt nach Lemma 1.12 für $x, x' \in \Omega(G)$ die Äquivalenz

$$\varphi_U(x) = \varphi_U(x') \ \forall U \leq G \iff x = x'.$$

Bemerkung 1.13 Für $U \leq G$ und eine G-Menge M gilt

(i) $\varphi_1(M) = |\{m \in M : 1m = m\}| = |M|$,

(ii) Falls $U \neq G$, $\varphi_G(G/U) = |\{gU \in G/U : GgU = gU\}| = 0$,

(iii) Falls $U = G$, $\varphi_G(G/U) = 1$.

Lemma 1.14 *Für $U, V \leq G$ gilt $\varphi_V(G/U) \neq 0$ genau dann, wenn ein $g \in G$ existiert mit $gVg^{-1} \subset U$. Ggf. erhält man*

$$\varphi_V(G/U) = |N_G(U) : U| \cdot |\{U' \text{ konjugiert zu } U : V \leq U'\}|.$$

Beweis: Die erste Aussage ist klar. Für $\varphi_V(G/U)$ gilt

$$\begin{aligned}\varphi_V(G/U) &= |\{gU \in G/U : g^{-1}VgU = U\}| \\ &= |\{gU \in G/U : V \subset gUg^{-1}\}| \\ &= \frac{1}{|U|} \cdot |\{g \in G : V \subset gUg^{-1}\}| \\ &= \sum_{g \in G} \frac{1}{|U|} \cdot \mathbb{1}_{gUg^{-1}}(V) \\ &= \sum_{K \in C_G(U)} \frac{|N_G(K)|}{|U|} \cdot \mathbb{1}_K(V) \\ &= |N_G(U) : U| \cdot |\{U' \text{ konjugiert zu } U : V \leq U'\}|,\end{aligned}$$

wobei die letzte Gleichung durch $N_G(hUh^{-1}) = hN_G(U)h^{-1}$ folgt. □

Bemerkung 1.15 Sei $x \in \Omega(G)$. Nach Lemma 1.14 und dem Beweis von Lemma 1.12 ist eine Untergruppe $U \leq G$ eine maximale Untergruppe mit $\mu_U(x) \neq 0$ genau dann, wenn U eine maximale Untergruppe mit $\varphi_U(x) \neq 0$ ist. Ggf. ist

$$\varphi_U(x) = \mu_U(x) \cdot \varphi_U(G/U) = \mu_U(x) \cdot |N_G(U) : U|.$$

2 Anwendung auf endlichen Gruppen

Bemerkung 2.1 Stets sei $C \coloneqq C_n$ die zyklische Gruppe der Ordnung n und G eine beliebige Gruppe gleicher Ordnung.

Satz 2.2 *Es exisitert ein Ring Homomorphismus $\alpha\colon \Omega(C) \to \Omega(G)$, sodass für jede Untergruppe $U \leq G$ und jedes $x \in \Omega(C)$ die Gleichheit*

$$\varphi_U(\alpha(x)) = \varphi_{C_{|U|}}(x)$$

gilt. Das heißt die Anzahl der U-invarianten Elemente der G-Menge (bzw. Klasse) $\alpha(x)$ entspricht der Anzahl $C_{|U|}$-invarianten Elemente der C-Menge (bzw. Klasse) x.

Beweis: Für den Beweis wird auf [DSY92] verwiesen. □

Bemerkung 2.3 Die Abbildung α in Satz 2.2 heißt Frobenius-Wielandt Homomorphismus. Da φ injektiv ist, können wir Elemente $x \in \Omega(C)$ mithilfe von $\varphi(x)$ charakterisieren. Mithilfe der Existenz von α können wir dies auf $\Omega(G)$ übertragen. Im Folgenden werden wir zunächst einige Aussagen für $x_d \coloneqq \alpha(C/C_{|G|/d}) \in \Omega(G)$, für einen Teiler d der Gruppenordnung $|G|$, treffen. Insbesondere kann man bei passender Wahl von d auf die Existenz und Anzahl von p-Untergruppen schließen. Sowie einige weitere Kongruenzen herleiten.

Lemma 2.4 *Für jeden Teiler d von $|G|$ gilt*

$$\varphi_U(x_d) = \begin{cases} d & \text{falls } d \mid |G:U|, \\ 0 & \text{sonst.} \end{cases}$$

Beweis: Nach Satz 2.2 gilt

$$\varphi_U(x_d) = \varphi_{C_{|U|}}(C/C_{|G|/d}).$$

Weiter sei $C_{|U|} \leq C_{|G|/d}$, d.h $\exists a \in \mathbb{N} : a|U| = |G|/d$ bzw. $ad = |G|/|U| = |G:U|$. Offenbar gilt dann $gC_{|G|/d} = C_{|G|/d}\ \forall g \in C_{|U|}$. Folglich gilt

$$\begin{aligned} \varphi_{C_{|U|}}(C/C_{|G|/d}) &= |(C/C_{|G|/d})^{C_{|U|}}| \\ &= |\{cC_{|G|/d} \in C/C_{|G|/d} : gcC_{|G|/d} = c(gC_{|G|/d}) = cC_{|G|/d}\ \forall g \in C_{|U|}\}| \\ &= |C : C_{|G|/d}| = d. \end{aligned}$$

Nun sei $C_{|U|} \not\leq C_{|G|/d}$ oder äquivalent nach analogen Überlegungen $d \nmid |G:u|$. Dementsprechend existiert ein $g \in C_{|U|}$ mit $g \notin C_{|G|/d}$. Insbesondere ist $g^{-1} \notin C_{|G|/d}$. Somit ist $gC_{|G|/d} \neq C_{|G|/d}$. Damit existiert für jedes $cC_{|G|/d} \in C/C_{|G|/d}$ ein $g \in C_{|U|}$ mit $gcC_{|G|/d} = cgC_{|G|/d} \neq cC_{|G|/d}$. Also ist $\varphi_U(C/C_{|G|/d}) = 0$. □

Bemerkung 2.5 Wir möchten $x_d \in \Omega(G)$ als Summe $x_d = \sum'_{U \leq G} \mu_U(x_d)G/U$ darstellen. Die Vorfaktoren sind nach Lemma 1.7 eidneutig. Des Weiteren ist φ injektiv nach Lemma 1.12, d.h finden wir ein Element $x \in \Omega(G)$, sodass $\varphi_U(x) = \varphi_U(x_d)$ für alle $U \leq G$ gilt, so ist $x = x_d$. Nun ist $\varphi_U(x_d) = 0$, für alle $U \leq G$ mit $d \nmid |G:U|$. Folglich können wir $x = \sum'_{U \leq G, d \| G:U|} \mu_U(x_d)G/U$ wählen und erhalten durch die Injektivität $x = x_d$. Also ist $\mu_U(x_d) = 0$, außer für $d \mid |G:U|$.

Lemma 2.6 *Sei $U \leq G$ eine beliebige Untergruppe. Sei $d = |G:U|$, so folgt*

$$\mu_U(x_d) = |G : N_G(U)| = |\{gUg^{-1} : g \in G\}|.$$

Beweis: Nehmen wir an es gäbe eine Untergruppe $H \leq G$ mit $|G:H| = d$ und $U \leq gHg^{-1}$ für ein $g \in G$. Insbesondere ist der Index von H minimal, sodass $\mu_H(x_d) \neq 0$ gilt, d.h $|H|$ ist maximal, sodass $\mu_H(x_d) \neq 0$. Nun gilt bereits $|U| = |H|$. Somit sind U und H zueinander konjugiert. Daher ist U eine maximale Untergruppe von G mit $\mu_U(x_d) \neq 0$. Man erhält mit Bemerkung 1.15 und Lemma 2.4

$$\mu_U(x_d) = \frac{\varphi_U(x_d)}{|N_G(U):U|} = \frac{d}{|N_G(U):U|} = \frac{|G:U|}{|N_G(U):U|} = |G : N_G(U)|$$

die Anzahl der Untergruppen von G, die zu U konjugiert sind. □

Satz 2.7 (Sylow) *Sei $|G| = dp^n$ für eine Primzahl p, dann existiert eine Untergruppe $U \leq G$ mit Index d, d.h der Ordnung p^n.*

Beweis: Sei $x_d \in \Omega(G)$ wie in Bemerkung 2.5. Wir schreiben x_d in der Form

$$x_d = \sum_{U \leq G}{}' \mu_u(x_d)G/U = \sum_{U \leq G, d \| G:U|}{}' \mu_U(x_d)G/U.$$

Nun betrachte $\varphi_1(x_d)$ und erhalte

$$d = \sum_{U \leq G, d || G:U|}{}' \mu_U(x_d)|G:U|.$$

Sei $ad = |G:U|$ für $a \in \mathbb{N}$. Nun teilt $|G:U|$ die Gruppenordnung $|G| = dp^n$. Daher $p \mid a$ oder $a = 1$. Wir erhalten

$$\sum_{U \leq G, d || G:U|}{}' \mu_U(x_d)|G:U| \equiv \sum_{U \leq G, d = |G:U|}{}' \mu_U(x_d)|G:U| \equiv d \not\equiv 0 \mod pd.$$

Demnach existiert eine Untegruppe U mit Index d. □

Bemerkung 2.8 Sei $K \leq G$ eine p-Untergruppe, sowie $U \leq G$ eine p-Sylowgruppe, d.h $p \nmid |G:U|$, dessen Existenzen nach Satz 2.7 folgen. Die Bahnenlängen der Operation von K auf G/U sind Teiler von $|K|$, d.h p-Potenzen. Daher ist die Anzahl der Fixpunkte von G/U unter K, also die Anzahl der Bahnen der Länge 1, kongruent modulo p zu der Anzahl der Elemente auf denen K operiert. Man erhält somit

$$\varphi_K(G/U) \equiv |G:U| \not\equiv 0 \mod p.$$

Nach Lemma 1.14 existiert ein $g \in G$ mit $gKg^{-1} \subset U$. Somit sind je zwei p-Sylowgruppen von G konjugiert. Außerdem ist jede p-Untergruppe von G in einer p-Sylowgruppe enthalten.

Satz 2.9 (Sylow, Frobenius) *Sei $G = dp^n$. So ist die Anzahl der Untergruppen $U \leq G$ der Ordnung p^n kongruent zu 1 modulo p.*

Beweis: Wie im Beweis von Satz 2.7, erhalten wir die Gleichung

$$d = \sum_{U \leq G, d || G:U|}{}' \mu_U(x_d)|G:U| = \sum_{U \leq G, |U| || p^n}{}' \mu_U(x_d)|G:U|.$$

Teilen wir durch d erlangen wir

$$\begin{aligned} 1 &= \sum_{U \leq G, |U| || p^n}{}' \mu_U(x_d)\frac{|G:U|}{d} \\ &= \sum_{U \leq G, |U| || p^n}{}' \mu_U(x_d)\frac{p^n}{|U|} \\ &\equiv \sum_{U \leq G, |U| = p^n}{}' \mu_U(x_d) \mod p \end{aligned}$$

Für $|U| = p^n$ bzw. $d = \frac{|G|}{p^n} = |G:U|$ folgt nach Lemma 2.6 $\mu_U(x_d) = |G:N_G(U)| = |\{gUg^{-1} : g \in G\}|$. Demnach gilt

$$1 \equiv \sum_{U \leq G, |U| = p^n}{}' \mu_U(x_d) \;=\; \sum_{U \leq G, |U| = p^n}{}' |\{gUg^{-1} : g \in G\}| = |\{U \leq G : |U| = p^n\}| \mod p.$$

□

Lemma 2.10 (Cauchy, Frobenius, Burnside) *Für jedes $x \in \Omega(G)$ gilt die* Cauchy-Frobenius-Burnside Kongruenz

$$\sum_{g \in G} \varphi_{<g>}(x) \equiv 0 \mod |G|.$$

Beweis: Sei $U \leq G$ und $x = G/U$. Dann gilt

$$\begin{aligned}
\sum_{g \in G} \varphi_{<g>}(G/U) &= \sum_{g \in G} |\{hU \in G/U : ghU = hU\}| \\
&= \sum_{g \in G, hU \in G/U} \mathbb{1}_{\{ghU\}}(hU) \\
&= \sum_{hU \in G/U} \sum_{g \in G} \mathbb{1}_{\{ghU\}}(hU) \\
&= \sum_{hU \in G/U} |\{g \in G : ghU = hU\}| \\
&= \sum_{hU \in G/U} |\{g \in G : \exists u \in U \text{ with } g = huh^{-1}\}| \\
&= \sum_{hU \in G/U} |hUh^{-1}| \\
&= |G : U| \cdot |U| = |G| \equiv 0 \mod |G|.
\end{aligned}$$

Offenbar folgt die Behauptung für beliebiges $x = \sum'_{U \leq G} \mu_U(x) G/U$. □

Satz 2.11 (Frobenius) *Sei m ein Teiler von $|G|$. Dann gilt*

$$|\{g \in G : g^m = 1\}| \equiv 0 \mod m.$$

Beweis: Wir betrachten wieder x_d und definieren $d := |G|/m$. Nach Lemma 2.10 gilt

$$\sum_{g \in G} \varphi_{<g>}(x_d) \equiv 0 \mod |G| = dm. \tag{1}$$

Außerdem gilt

$$\begin{aligned}
\sum_{g \in G} \varphi_{<g>}(x_d) &= \sum_{g \in G, d || G:<g>|} d \\
&= \sum_{g \in G, |g| | m} d \\
&= d \cdot |\{g \in G : g^m = 1\}|.
\end{aligned}$$

Teilen wir nun durch d, folgt mit Gleichung (1)

$$|\{g \in G : g^m = 1\}| = \frac{1}{d} \sum_{g \in G} \varphi_{<g>}(x_d) \equiv 0 \mod m.$$

□

Literatur

[DSY92] A. Dress,C. Siebeneicher, T. Yoshida, *An Application of Burnside Rings in Elementary Finite Group Theory*, Adv. in Math., Vol. 91, 1992.

[Die79] T. tom Dieck, D.A. Buchsbaum, *Transformation Groups and Representation Theory*, Lecture Notes in Math., Vol. 766, Berlin 1979.