Burnside-Ringe

Vortrag im Rahmen des Seminars zur Computeralgebra

Oliver Braun, Sebastian Schönnenbeck

Wintersemester 2010/11

2. Grundlagen und der Burnside-Ring

2.0.1. Definition: G-Mengen und Ähnlichkeit

Operiert eine Gruppe G auf einer Menge M durch eine Operation ω, so nennt man (M, ω) (bzw. oft auch nur M) eine G-Menge.
Zwei G-Mengen M, N heißen ähnlich, falls es eine bijektive Abbildung φ zwischen ihnen gibt, sodass $\varphi(gm) = g\varphi(m)$ für alle $g \in G,\ m \in M$ gilt. φ heißt dann eine Ähnlichkeit von G-Mengen. Die Eigenschaft $\varphi(gm) = g\varphi(m)$ nennt man G-Äquivarianz von φ.

2.0.2. Definition: Diagonale Operation

Operiert G auf den Mengen M und N, so operiert G ebenfalls auf $M \times N$ durch $g(m, n) := (gm, gn)$. Diese Operation nennt man diagonale Operation.

2.0.3. Satz: Hauptsatz über transitive G-Mengen

Die Ähnlichkeitsklassen der transitiven G-Mengen und die Konjugiertenklassen von Untergruppen von G stehen zueinander in Bijektion.

2.1. Markentafeln

2.1.1 Definition: Fixpunkte

Operiert eine Gruppe G auf einer Menge M, so definieren wir

$$\mathrm{fix}_G(M) := \{m \in M \mid gm = m\ \forall g \in G\}$$

2.1.2. Lemma

Für zwei Untergruppen U_i, U_j einer Gruppe G gilt:

Es existiert ein Fixpunkt von U_i auf $G/U_j \Leftrightarrow U_i$ ist konjugiert zu einer Untergruppe von U_j.

Außerdem ist $\mathrm{fix}_{U_i}(G/U_j)$ konstant auf der Konjugiertenklasse von U_i vermöge $\mathrm{fix}_{xU_ix^{-1}}(G/U_j) = x\,\mathrm{fix}_{U_i}(G/U_j)$.

2.1.3. Korollar

1. Notwendig für die Existenz eines Fixpunktes ist $|U_j|\big||U_i|$.
2. $U_j \leq U_i \Rightarrow$ Es existiert mindestens ein Fixpunkt.
3. Für $U, V \leq G$ mit $U \cong V$ und $U \not\sim V$ gilt $\mathrm{fix}_V(G/U) = \emptyset$.

4. Für $U \leq G$ gilt $\mathrm{fix}_U(G/U) = N_G(U)/U$.

5. $V \leq U \trianglelefteq G \Rightarrow \mathrm{fix}_V(G/U) = G/U$.

2.1.4. Definition: Markentafel

$|G| < \infty$: $(M(G))_{ij} := (|\,\mathrm{fix}_{U_j}([G/U_i])|)_{1\leq i,j\leq k}$, die Markentafel von G.
Dabei U_i ein Vertretersystem der Konjugiertenklassen von Untergruppen von G mit $U_1 = \{1\}$, $U_k = G$ und $|U_i| \leq |U_j|$, falls $i < j$.
Die Anzahl der Fixpunkte auf einer Konjugiertenklasse ist konstant und die Markentafel somit wohldefiniert.

2.2. Verbände und Abzählringe

2.2.1. Definition: Verband

Eine Menge $\mathcal{V}$ mit den zwei Verknüpfungen $\vee, \wedge$ heißt Verband, falls für alle $u, v, w \in \mathcal{V}$ gilt:

1. $u \vee (v \vee w) = (u \vee v) \vee w$ und $u \wedge (v \wedge w) = (u \wedge v) \wedge w$

2. $u \vee v = v \vee u$ und $u \wedge v = v \wedge u$

3. $u \vee (u \wedge v) = u$ und $u \wedge (u \vee v) = u$

4. $u \vee u = u,\ u \wedge u = u$

Auf einem Verband $(\mathcal{V}, \vee, \wedge)$ lässt sich durch $v \leq w :\Leftrightarrow v \wedge w = v$ eine partielle Ordnung definieren.

2.2.3. Definition: Halbgruppenring

$(M, \cdot)$ endliche Halbgruppe,

$$\mathbb{Z}M = \left\{ \sum_{m\in M} a_m m \mid a_m \in \mathbb{Z},\ a_m \neq 0 \text{ nur für endlich viele m} \right\}$$

mit der Addition $\sum\limits_{m\in M} a_m m + \sum\limits_{m\in M} b_m m = \sum\limits_{m\in M} (a_m + b_m) m$ und der Multiplikation $\left(\sum\limits_{m\in M} a_m m\right)\left(\sum\limits_{m\in M} b_m m\right) = \sum\limits_{m\in M}\sum\limits_{st=m} a_s b_t m$.

2.2.4. Lemma: Operation auf dem Halbgruppenring

Operiert eine Gruppe G durch Automorphismen auf der Halbgruppe M, so operiert G auch durch Ringautomorphismen auf $\mathbb{Z}M$.

2.2.5. Satz: Definition und Eigenschaften des Fixrings

Die Gruppe G operiere so durch Automorphismen auf der Halbgruppe M, dass die Bahnen der Operation endlich sind. Dann ist $\mathrm{fix}_G(\mathbb{Z}M)$ ein Teilring von $\mathbb{Z}M$ und wir nennen $\mathrm{fix}_G(\mathbb{Z}M)$ den Fixring des Halbgruppenringes $\mathbb{Z}M$.
$\mathrm{fix}_G(\mathbb{Z}M)$ hat als $\mathbb{Z}$-Modulbasis die so genannten Bahnsummen $\overline{B} := \sum\limits_{m\in B} m$ der Bahnen der Operation von G auf M und es gilt $\mathrm{fix}_G(\mathbb{Z}M) = \bigoplus\limits_{B\in M/G} \mathbb{Z}\overline{B}$.
Wir multiplizieren in $\mathrm{fix}_G(\mathbb{Z}M)$ durch $\overline{B}\cdot\overline{C} = \sum_{D\in M/G} \mu_{B,C}^D \overline{D}$, wobei $\mu_{B,C}^D = |\{(m,n) \in B \times C \mid m \cdot n = d\}| \in \mathbb{Z}$ mit einem beliebig aber fest gewählten $d \in D$ gilt.
Einen Ring, der isomorph zu $\mathrm{fix}_G(\mathbb{Z}M)$ ist und eine wie hier beschriebene Basis besitzt, nennen wir den G-Abzählring von M oder auch den $(M, \cdot, G)$-Abzählring.

2.2.6. Satz: $R^\vee$ und $R^\wedge$

Sei $(\mathcal{V}, \wedge, \vee)$ ein endlicher Verband und $\leq$ eine partielle Ordnung auf $\mathcal{V}$. Die Gruppe G operiere auf $\mathcal{V}$ durch Verbandsautomorphismen. Es seien zudem $(B_i)_{i\in\underline{s}}$ die Bahnen auf $\mathcal{V}$ unter G. Dabei sei B_1 das minimale und B_s das maximale Element des Verbandes (bezüglich $\leq$). Zudem ordnen wir die Bahnen Œ so an, dass aus $v \in B_i$, $w \in B_j$ und $v \leq w$ folgt, dass $i \leq j$.

1. Der $(\mathcal{V}, \wedge, G)$-Abzählring habe die Basis $(b_i^\wedge)_{i\in\underline{s}}$ entsprechend den $(B_i)_{i\in\underline{s}}$ (vgl. 2.2.5.). Dann ist $R^\wedge \cong \bigoplus_{i=1}^{s} \mathbb{Z}$ (mit komponentenweiser Addition und Multiplikation) durch den Isomorphismus
$$b_i^\wedge \mapsto (\alpha_{i1}^\wedge, ..., \alpha_{is}^\wedge) \text{ mit } \alpha_{ij}^\wedge = |\{x \in B_i \mid x \leq y\}| \text{ für ein festes } y \in B_j.$$
2. Analog habe der $(\mathcal{V}, \vee, G)$-Abzählring $R^\vee$ die Basis $(b_i^\vee)_{i\in\underline{s}}$. Dann ist $R^\vee \cong \bigoplus_{i=1}^{s} \mathbb{Z}$ durch den Isomorphismus
$$b_i^\vee \mapsto (\alpha_{i1}^\vee, ..., \alpha_{is}^\vee) \text{ mit } \alpha_{ij}^\vee = |\{x \in B_i \mid y \leq x\}| \text{ für ein festes } y \in B_j.$$
3. Es gilt $\alpha_{ij}^\vee |B_j| = \alpha_{ji}^\wedge |B_i|$ und $|B_i| = \alpha_{is}^\vee = \alpha_{i1}^\wedge$.

2.3. Der Burnside-Ring

2.3.1. Definition: Burnside-Ring

Es sei G eine endliche Gruppe. Auf der Menge $\hat{G}$ der Ähnlichkeitsklassen $[M]$ der endlichen G-Mengen M definieren wir die folgenden Verknüpfungen:

$$\hat{G} \times \hat{G} \to \hat{G} \ : \ [M] + [N] := [M \,\dot\cup\, N] \text{ mit } M \cap N = \emptyset$$
$$\hat{G} \times \hat{G} \to \hat{G} \ : \ [M] \cdot [N] := [M \times N]$$

$(\hat{G}, +, \cdot)$ kommutativer Halbring mit $0 = [\emptyset]$ und $1 = [\{1\}]$.

Auf $\hat{G} \times \hat{G}$ definieren wir nun die Äquivalenzrelation $\sim$:

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

$([M], [N]) := [M] - [N]$, $([M], [\emptyset]) := [M]$ und $([\emptyset], [M]) := -[M]$. Definiere den Burnside-Ring von G als $B(G) := (\hat{G} \times \hat{G})/\sim$.

$B(G)$ machen wir mittels der zwei folgenden Verknüpfungen zu einem Ring:

$$([M_1] - [M_2]) + ([N_1] - [N_2]) := ([M_1] + [N_1]) - ([M_2] + [N_2])$$

$$([M_1] - [M_2]) \cdot ([N_1] - [N_2]) := ([M_1] \cdot [N_1] + [M_2] \cdot [N_2]) - ([M_1] \cdot [N_2] + [M_2] \cdot [N_1])$$

Zudem können wir $\hat{G}$ in $B(G)$ einbetten durch $\hat{G} \hookrightarrow B(G) \ : \ [M] \mapsto [M] := [M] - [\emptyset]$, d.h. die Abbildung ist injektiv und verträglich mit $+$ und $\cdot$.

$B(G)$ ist ein freier $\mathbb{Z}$-Modul mit Basis $\mathcal{B} := \{[G/U] \mid U \in \mathcal{V}\}$, wobei $\mathcal{V}$ ein Vertretersystem der Konjugiertenklassen von Untergruppen von G ist.

2.3.2. Satz: $R^\wedge$ und der Burnside-Ring

G endliche Gruppe, $(B_i)_{i\in\underline{s}}$ Familie der Konjugiertenklassen von Untergruppen von G, $(U_i)_{i\in\underline{s}}$ mit $U_i \in B_i \forall i$ Vertretersystem, $(M_i)_{i\in\underline{s}}$ mit $M_i \cong G/U_i$ (als G-Menge) Vetretersystem der Ähnlichkeitsklassen transitiver G-Mengen. Sei $R^\wedge(G)$ der

Abzählring des Untergruppenverbands von G mit $\cap$ und der Konjugation als Operation mit einer geeigneten Basis $(b_i^\wedge)_{i\in\underline{s}}$ bezüglich der U_i. In der Sprache von Satz 2.2.5. also $b_i^\wedge = \sum_{V\in B_i} V$.

Dann gilt:

$$\phi : B(G) \to R^\wedge(G); [M_i] \mapsto n_i \cdot b_i^\wedge$$

ist ein Ringmonomorphismus, wobei wir $n_i := |N_G(U_i)/U_i|$ setzen.

3. Abzählprobleme

3.0.3. Definition: Färbungen und Farbenzähler

G endliche Gruppe, M, F endliche G-Mengen. G op. auf F^M vermöge

$$G \times F^M \to F^M,\ (g, f) \mapsto f \circ \overline{g}^{-1}$$

Dabei ist $\overline{g}$ die durch g auf M induzierte Permutation.
Jede Bahn von F^M unter G nennen wir nun eine Färbung (mit Farbenmenge F).

Da F endlich ist, können wir die Elemente auffassen als Variablen $x_1, ..., x_n$ im Polynomring $\mathbb{Z}[x_1, ..., x_n]$. Dann ist die Abbildung

$$\psi\ :\ F^M \to \mathbb{Z}[x_1, ..., x_n],\ f \mapsto \prod_{m\in M} f(m)$$

offensichtlich G-invariant und wir nennen sie den Farbenzähler von f.
Ist $Gf \subseteq F^M$ mit $\psi(f) = x_1^{a(1)} \cdots x_n^{a(n)}$ eine Färbung, so sagen wir Gf ist vom Färbungstyp $x_1^{a(1)} \cdots x_n^{a(n)}$.

3.0.4. Lemma: U-Fixpunkte auf F^M

$f \in F^M$ fix unter $U \leq G \Leftrightarrow f$ konstant auf den U-Bahnen von M (die Anzahl der U-Fixpunkte ist also $|F|^{|M/U|}$). Genauer: die Anzahl der U-Fixpunkte in $\psi^{-1}(\{x_1^{a(1)} \cdots x_n^{a(n)}\})$ ist gleich dem Koeffizienten von $x_1^{a(1)} \cdots x_n^{a(n)}$ in dem Polynom

$$p_U = p_U(x_1, ..., x_n) := \prod_{j=1}^{\alpha} \sum_{i=1}^{n} x_i^{\lambda(j)}$$

Dabei habe U genau α Bahnen auf M, deren Längen mit $\lambda(j),\ j \in \underline{\alpha}$ bezeichnet seien.

3.0.5. Satz

$(U_i)_{i\in\underline{s}}$ Vertretersystem der Konjugiertenklassen von Untergruppen von G, $p_i := p_{U_i}$ wie in 3.0.4. Dann sei

$$\begin{aligned} q &:= \sum_{a(1)+\cdots+a(n)=|M|} \left[\psi^{-1}(\{x_1^{a(1)} \cdots x_n^{a(n)}\})\right] x_1^{a(1)} \cdots x_n^{a(n)} \\ &= \sum_{a(1)+\cdots+a(n)=|M|} \left(\sum_{i=1}^{s} r_{a(1),...,a(n);i}[G/U_i]\right) x_1^{a(1)} \cdots x_n^{a(n)} \qquad (*) \\ &= \sum_{i=1}^{s} \underbrace{\sum_{a(1)+\cdots+a(n)=|M|} r_{a(1),...,a(n);i} x_1^{a(1)} \cdots x_n^{a(n)}[G/U_i]}_{q_i} \end{aligned}$$

(*): stelle $\psi^{-1}(\{x_1^{a(1)} \cdots x_n^{a(n)}\})$ als Linearkombination in der Standardbasis von $B(G)$ dar.

das Element von $B(G)[x_1, ..., x_n]$, das die Anzahl $r_{a(1),...,a(n);i}$ der Färbungen vom Äquivalenztyp $[G/U_i]$ mit Färbungstyp $x_1^{a(1)} \cdots x_n^{a(n)}$ angibt. Identifiziert man nun wie üblich $[G/U_i]$ mit der i-ten Zeile der Markentafel $M(G)$ von G, so gilt

1. $(q_1, ..., q_s) = (p_1, ..., p_s)(M(G))^{-1}$

2. Die $\lambda(\ell) = \lambda(i,\ell)$ von U_i auf M (aus den p_i) liest man ab aus

$$[M][G/U_i] = \sum_{\ell=1}^{s} m_{i,\ell}[G/U_\ell]$$

mit $\lambda(i,\ell) := \frac{|G/U_\ell|}{|G/U_i|} = \frac{|U_i|}{|U_\ell|}$ mit Vielfachheit $m_{i,\ell}$, d.h.

$$p_i = \prod_{i=1}^{s} \left(\sum_{r=1}^{n} x_r^{\lambda(i,\ell)} \right)^{m_{i,\ell}}$$

für $i = 1, ..., s$. Dabei ist $m_{i,\ell} = 0$, falls $\lambda(i,\ell)$ nicht ganzzahlig ist.

Zur Struktur des Burnside-Rings

4.0.7. Satz: Primideale im Burnside-Ring

G endliche Gruppe, $(U_i)_{1 \leq i \leq s}$ Vertretersystem der Konjugiertenklassen von Untergruppen. Ein Ideal $I \trianglelefteq B(G)$ ist Primideal genau dann, wenn ein $i \in \underline{s}$ und ein $p \in \mathbb{P} \cup \{0\}$ existieren, sodass $I = \{x \in B(G) \mid |\operatorname{fix}_{U_i}(x)| \in p\mathbb{Z}\}$.

4.0.8. Satz: Der Burnside-Ring des direkten Produkts

Seien G und H zwei endliche Gruppen von teilerfremder Ordnung. Dann gilt:

$$B(G \times H) = B(G) \otimes B(H)$$