Algebraische Zahlentheorie II
Sommersemester 2022

Dr. Katharina Hübner
basierend auf Alexander Schmidts AZT2-Skript von 2014

Inhaltsverzeichnis

1 Gruppenhomologie

1.1 Der Gruppenring

Sei G eine Gruppe und A ein kommutativer Ring.

Definition. Der **Gruppenring** $A[G]$ besteht aus allen formalen Linearkombinationen

$$\sum_{g \in G} a_g \cdot g, \qquad a_g = 0 \text{ für fast alle } g \in G.$$

Addition: Komponentenweise.
Multiplikation: $(ag) \cdot (b \cdot h) = ab \cdot gh$ und linear fortsetzen. Das Element $1_A \cdot e_G$ ist die 1 im Ring $A[G]$. Der Ring $A[G]$ ist genau dann kommutativ, wenn G dies ist. Ein Gruppenhomomorphismus $f : G \to H$ induziert einen Ringhomomorphismus $A[G] \to A[H]$, $\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g f(g)$. Der Spezialfall $H = 1$ hat einen eigenen Namen:

Definition. Der Ringhomomorphismus

$$\varepsilon_A \colon A[G] \longrightarrow A \quad , \quad \sum a_g g \longmapsto \sum a_g,$$

heißt die **Augmentation(sabbildung)**. $I_G^A := \ker(\varepsilon_A)$ heißt das **Augmentationsideal**.

Lemma 1.1. *Das Augmentationsideal $I_G^A \subset A[G]$ ist als A-Modul frei über der Basis*

$$\{g - 1 \mid g \in G \smallsetminus \{e\}\}.$$

Ist $S \subset G$ ein Erzeugendensystem, so erzeugt die Menge $S - 1 = \{s - 1 \mid s \in S\}$ I_G^A als $A[G]$-Links(Rechts-)ideal.

Beweis. Die Elemente $g-1$, $g \in G \smallsetminus \{e\}$, liegen in I_G^A und sind linear unabhängig über A. Sei $\alpha = \sum\limits_{i=1}^{n} a_i g_i \in I_G^A$. Dann gilt $\sum a_i = 0$, also $\alpha = \sum a_i(g_i - 1)$. Wegen $e - 1 = 0 \in A[G]$ folgt die erste Aussage. Für die zweite genügt es zu zeigen, dass für alle $g \in G$ das Element $g - 1$ im von $S - 1$ erzeugten Linksideal liegt. Wegen $s_1 s_2 - 1 = s_1(s_2 - 1) + s_1 - 1$ und

$$s^{-1} - 1 = -s^{-1}(s - 1)$$

folgt dies aus der Existenz einer Darstellung

$$g = s_1^{\pm 1} \cdot s_2^{\pm 1} \dots s_n^{\pm 1}, \quad s_i \in S.$$

□

Definition. Für $g, h \in G$ heißt $[g, h] = ghg^{-1}h^{-1}$ der **Kommutator** von g und h (oft in der Literatur auch $(g, h) = g^{-1}h^{-1}gh$.) Die durch alle Kommutatoren erzeugte Untergruppe $[G, G]$ heißt die **Kommutatorgruppe**.

Lemma 1.2. *$[G, G]$ ist ein Normalteiler in G. Die Faktorgruppe $G^{\mathrm{ab}} = G/[G, G]$ ist abelsch.*

Beweis. Für $[G, G] \lhd G$ genügt es zu zeigen, dass für $g, h_1, h_2 \in G$ gilt $g[h_1, h_2]g^{-1} \in [G, G]$. Dies ist klar wegen

$$\begin{aligned} g[h_1, h_2]g^{-1} &= gh_1h_2h_1^{-1}h_2^{-1}g^{-1} \\ &= gh_1g^{-1}gh_2g^{-1} \cdot gh_1^{-1}g^{-1}gh_2^{-1}g^{-1} \\ &= [gh_1g^{-1}, gh_2g^{-1}]. \end{aligned}$$

Wegen $gh(hg)^{-1} = [g, h] \in [G, G]$ ist $G^{\mathrm{ab}} = G/[G, G]$ abelsch. □

Bemerkung. Der Funktor $G \mapsto G^{\mathrm{ab}}$ ist linksadjungiert zur natürlichen Inklusion $\mathcal{A}b \subset$ (Groups).

Wir betrachten die Untergruppe $I_G^2 = I_G \cdot I_G$ in $I_G = I_G^{\mathbb{Z}}$.

Satz 1.3. *Für $I_G = I_G^{\mathbb{Z}} \subset \mathbb{Z}[G]$ gilt $I_G/I_G^2 \cong G^{\mathrm{ab}}$.*

Beweis. Wir betrachten die Abbildung

$$\varphi\colon G \longrightarrow I_G/I_G^2 \quad , \quad g \longmapsto g-1.$$

Wegen $gh - 1 = (g-1) + (h-1) + \underbrace{(g-1)(h-1)}_{\in I_G^2}$
ist φ ein Gruppenhomomorphismus. Da I_G/I_G^2 abelsch ist, gilt $\varphi([G,G]) = 0$. Dies induziert $\tilde{\varphi}\colon G^{\mathrm{ab}} \to I_G/I_G^2$. Wir konstruieren die inverse Abbildung. Nach 1.1 ist I_G der freie $\mathbb{Z}$-Modul über der Menge $W = \{g-1 \mid g \neq e\}$. Die Abbildung $W \to G^{\mathrm{ab}}$, $(g-1) \mapsto g[G,G]$ setzt sich daher eindeutig zu einem Homomorphismus abelscher Gruppen $\psi\colon I_G \to G^{\mathrm{ab}}$ fort. Wegen $(g-1)(h-1) = (gh-1) - (g-1) - (h-1)$ gilt

$$\psi((g-1)(h-1)) = gh[G,G] \cdot (g[G,G])^{-1} \cdot (h[G,G])^{-1} = 1,$$

also induziert ψ einen Homomorphismus $\tilde{\psi}\colon I_G/I_G^2 \to G^{\mathrm{ab}}$. Schließlich sind $\tilde{\psi}$ und $\tilde{\varphi}$ zueinander invers. □

1.2 G-Moduln

Definition. Ein ***G*-Links-Modul** A ist eine abelsche Gruppe A zusammen mit einer Operation $G \times A \to A$, $(g,a) \mapsto ga$ mit $g(a_1 + a_2) = ga_1 + ga_2$, $gh(a) = g(h(a))$ und $ea = a$ für alle $a \in A$. G-Rechtsmoduln definiert man analog.

Bemerkung. Ein G-Links(Rechts)modul ist nichts anderes als ein $\mathbb{Z}[G]$-Links -(Rechts)modul.

Ist A ein G-Rechtsmodul, so können wir durch $ga \overset{\mathrm{df}}{=} ag^{-1}$ A auch als G-Linksmodul auffassen. M.a.W., es gilt

Lemma 1.4. *Die folgenden Kategorien sind natürlich äquivalent:*

(i) $\mathbb{Z}[G]$-*Linksmoduln.*
(ii) G-*Linksmoduln.*
(iii) G-*Rechtsmoduln.*
(iv) $\mathbb{Z}[G]$-*Rechtsmoduln.*

Beispiele. • $\mathbb{Z}[G]$ ist ein G-Modul.
• Sei L/K eine endliche Galoiserweiterung. Dann sind L^+ und $L^\times$ $\mathrm{Gal}(L/K)$-Moduln.

Im folgenden arbeiten wir immer mit Linksmoduln und machen, wann immer nötig, Rechtsmoduln zu Linksmoduln und umgekehrt.

Beispiele. • Für G-Linksmoduln A, B bilden wir das Tensorprodukt $A \otimes_G B$ indem wir A als G-Rechtsmodul auffassen und dann $A \otimes_{\mathbb{Z}[G]} B$ bilden. Anders gesagt:

$$A \otimes_G B = (A \otimes_{\mathbb{Z}} B)/\big((g^{-1}a, b) - (a, gb)\big).$$

• Ist A ein G-Linksmodul, so wird $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ zum G-Linksmodul durch $(g\varphi)(a) \colon = \varphi(g^{-1}a)$.

Definition. Wir nennen einen G-Modul **frei**, wenn er frei als $\mathbb{Z}[G]$-Modul ist.

Operationen auf G-Moduln

1) **Tensorprodukt:** $A \otimes_{\mathbb{Z}} B$ wird zum G-Modul durch $g(a \otimes b) = ga \otimes gb$.
2) **Homomorphismen:** $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ wird zum G-Modul durch $(g\varphi)(a) = g\varphi(g^{-1}a)$.
3) **Invarianten:**

$$A^G = \{a \in A \mid ga = a \quad \forall\, g \in G\}$$

heißt die (Unter)Gruppe der **(G-)Invarianten** von A.

Es gilt $\mathrm{Hom}_{\mathbb{Z}}(A, B)^G = \mathrm{Hom}_G(A, B)$

4) **Koinvarianten:**

$$A_G = A/\{(ga - a), g \in G, a \in A\} = A/I_G \cdot A$$

heißt die Gruppe der **Koinvarianten** von A.

Es gilt $(A \otimes_{\mathbb{Z}} B)_G = A \otimes_G B$.

Definition. Wir nennen einen G-Modul A **trivial**, wenn $ga = a \quad \forall\, g \in G$, $a \in A$.

Lemma 1.5. (i) *A^G ist der größte triviale Untermodul von A*

(ii) *A_G ist der größte triviale Faktormodul von A.*

Beweis. Klar. □

Sei nun $U \subset G$ eine Untergruppe. Wir betrachten den Vergissfunktor

$$\mathrm{Res}^G_U \colon G - \mathrm{Mod} \longrightarrow U - \mathrm{Mod}$$

Lemma 1.6. Res^G_U *überführt freie in freie und projektive in projektive Moduln.*

Beweis. Sei (x_i) ein Repräsentantensystem von Rechtsnebenklassen $U\backslash G$. Dann ist G die disjunkte Vereinigung der Mengen Ux_i. Für fixiertes i ist der U-Untermodul

$$M_i := \{ \sum_{g \in Ux_i} a_g g \mid a_g = 0 \text{ für fast alle } g\} \subset \mathbb{Z}[G]$$

isomorph zu $\mathbb{Z}[U]$, also frei. Daher ist

$$\mathrm{Res}_U^G \mathbb{Z}[G] \cong \bigoplus_i M_i$$

freier $\mathbb{Z}[U]$-Modul. Da Res_U^G mit der direkten Summe vertauscht, gilt Res_U^G (freier G-Modul) $=$ freier U-Modul. Ist nun P ein projektiver G-Modul so existiert ein (projektiver) G-Modul Q mit $P \oplus Q$ frei. Daher ist $\mathrm{Res}_U^G P$ direkter Summand im freien U-Modul $\mathrm{Res}_U^G (P \oplus Q)$, also projektiv. □

1.3 Homologie

Wir fassen $\mathbb{Z}$ als trivialen G-Modul auf. Dann gilt für jeden G-Modul A

$$A_G = (A \otimes_{\mathbb{Z}} \mathbb{Z})_G = A \otimes_G \mathbb{Z}.$$

Daher ist der Funktor

$$-_G \colon G - \mathrm{Mod} \longrightarrow \mathcal{A}b,\ A \longmapsto A_G,$$

rechtsexakt und es gilt

$$L_n(-_G)(A) = \mathrm{Tor}_n^{\mathbb{Z}[G]}(A, \mathbb{Z}).$$

Definition. $H_n(G, A) \stackrel{\mathrm{df}}{=} L_n(-_G)(A)$ heißt die ***n*-te Homologiegruppe von *G* mit Werten in *A***.

Wegen der Gleichheit $H_n(G, A) = \mathrm{Tor}_n^{\mathbb{Z}[G]}(A, \mathbb{Z})$ haben wir die folgenden Berechnungsmethoden:

1) Wähle projektive Auflösung $Q_\bullet \to A$. Dann gilt $H_n(G, A) = H_n((Q_\bullet)_G)$
2) oder wähle projektive Auflösung $P^\bullet \to \mathbb{Z}$. Dann gilt $H_n(G, A) = H_n(A \otimes_G P^\bullet)$.

Wir konstruieren nun eine freie Auflösung von $\mathbb{Z}$.
Setze für $n \geq 0$:

$$\begin{aligned} X_n &= \mathbb{Z}[G^{n+1}] = \mathbb{Z}[\overbrace{G \times \cdots \times G}^{n+1 \text{ Faktoren}}] \\ &= \{\text{freie ab. Gruppe über } (n+1)\text{-Tupel} \\ &\qquad (g_0, \ldots, g_n),\ g_i \in G,\ i = 0, \ldots, n\}, \end{aligned}$$

mit G-Modulstruktur gegeben durch

$$g(g_0, \ldots, g_n) = (gg_0, \ldots, gg_n).$$

- X_n ist ein freier G-Modul, Basis die $(n+1)$-Tupel der Form $(e, g_1, \ldots, g_n)$.
- Wir machen $X_\bullet$ zu einem Komplex indem wir G-Modulhomorphismen

$$d \colon X_{n+1} \longrightarrow X_n$$

durch $d((g_0, \ldots, g_{n+1})) = \sum\limits_{i=0}^{n+1} (-1)^i (g_0, \ldots, g_{i-1}, g_{i+1} \ldots g_{n+1})$ definieren.

Lemma 1.7. *$X_\bullet$ ist ein Komplex, d.h. $d \circ d = 0$.*

Beweis. Wir betrachten
$$d \circ d\colon X_{n+2} \longrightarrow X_n.$$
Es gilt
$$d \circ d((g_0, \ldots, g_{n+2})) = d\left(\sum_{i=0}^{n+2} (-1)^i (g_0, \ldots, \widehat{g_i}, \ldots, g_{n+2}\right)$$

$$= \sum_{j=0}^{n+1} (-1)^j \cdot \sum_{i=0}^{n+2} (-1)^i \overbrace{(g_0, \ldots, \widehat{g_i}, \ldots, g_{n+2})}^{\text{hieraus die j-te Komp. entfernen}} .$$
Für $j < i$ erhalten wir
$$(g_0, \ldots, \widehat{g_j}, \ldots, \widehat{g_i}, \ldots, g_{n+2}) \cdot (-1)^{i+j}.$$
Für $j \geq i$
$$(g_0, \ldots, \widehat{g_i}, \ldots, \hat{g}_{j+1}, \ldots, g_{n+2}) \cdot (-1)^{i+j}.$$
M.a.W.: Der Term $(g_0, \ldots, \widehat{g_a}, \ldots, \widehat{g_b}, \ldots, g_{n+2})$ $a < b$ taucht auf

für $j = a$, $i = b$ mit Vorfaktor $(-1)^{a+b}$ und
für $i = a$, $j = b - 1$ mit Vorfaktor $(-1)^{a+b-1}$. □

Lemma 1.8. *Es ist $\varepsilon \circ d_0\colon X_1 \xrightarrow{d_0} X_0 = \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z}$ die Nullabbildung.*

Beweis. Für $g_0, g_1 \in G$ beliebig gilt $\varepsilon \circ d_0((g_0, g_1)) = \varepsilon(g_1 - g_0) = 1 - 1 = 0$. □

Satz 1.9. *$X_\bullet \to \mathbb{Z}$ ist eine freie Auflösung von $\mathbb{Z}$ als G-Modul.*

Beweis. Wir setzen $d_{-1} = \varepsilon$. Z.z.: der Komplex
$$\cdots \to X_3 \longrightarrow X_2 \xrightarrow{d_1} X_1 \xrightarrow{d_0} X_0 \xrightarrow{d_{-1}} \mathbb{Z} \longrightarrow 0$$
ist exakt. Zum Beweis geben wir eine Nullhomotopie an, also Abbildungen $(D_i : X_i \to X_{i+1})$, $i \in \mathbb{Z}$, mit $d_i \circ D_i + D_{i-1} \circ d_{i-1} = \mathrm{id}_{X_i}$. Dann induzieren die homotopen Komplexhomomorphismen id und 0 die gleichen Abbildungen auf der Homologie, weshalb die Homologie Null und somit der Komplex exakt ist.

Nun setze $D_{-1} : \mathbb{Z} \to \mathbb{Z}[G]$, $1 \mapsto 1e$, und für $n \geq 0$:
$$D_n : X_n \longrightarrow X_{n+1},\ (g_0, \ldots, g_n) \longmapsto (e, g_0, \ldots, g_n).$$
Wir berechnen:
$$\begin{tikzcd}
X_3 \arrow[r] \arrow[d, shift left] \arrow[d, shift right] & X_2 \arrow[r] \arrow[d, shift left] \arrow[d, shift right] \arrow[dl, "D_2"] & X_1 \arrow[r, "d_0"] \arrow[d, shift left] \arrow[d, shift right] \arrow[dl, "D_1"] & X_0 \arrow[r, "d_{-1}"] \arrow[d, shift left] \arrow[d, shift right] \arrow[dl, "D_0"] & \mathbb{Z} \arrow[r] \arrow[d, shift left] \arrow[d, shift right] \arrow[dl, "D_{-1}"] & 0 \\
X_3 \arrow[r] & X_2 \arrow[r] & X_1 \arrow[r, "d_0"'] & X_0 \arrow[r, "d_{-1}"'] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

Zunächst gilt $d_{-1}D_{-1}(1) = \varepsilon(e) = 1$. Wir haben für $g \in G \subset X_0$

$$d_0 D_0(g) + D_{-1}d_{-1}(g) = d_0((e,g)) + D_{-1}(1) = g - e + e = g.$$

Für $n \geq 1$:

$d_n \circ D_n((g_0, \dots, g_n)) + D_{n-1} \circ d_{n-1}(g_0, \dots, g_n)$

$= d_n((e, g_0, \dots, g_n) + D_{n-1}\left(\sum_{i=0}^{n}(-1)^i(g_0, \dots, \widehat{g_i}, \dots, g_n)\right)$

$= \sum_{i=0}^{n+1}(-1)^i \overbrace{(e, g_0, \dots, g_n)}^{\text{i-te Komp. weg}} + \sum_{i=0}^{n}(-1)^i \overbrace{(e, g_0, \dots, g_n)}^{\text{i+1-te Komp. weg}}$

$= (g_0, \dots, g_n)$. □

Korollar 1.10. *Es gilt*

$$H_n(G, A) = H_n((A \otimes_{\mathbb{Z}} X_\bullet)_G).$$

Bemerkung. Man kann die Folgerung zur Definition machen. Dann muß man aber später vieles mühsam nachrechnen.

Satz 1.11. *Es gilt*

$$H_1(G, \mathbb{Z}) \cong G^{\mathrm{ab}}.$$

Beweis. Wir betrachten die exakte Folge

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

Da $\mathbb{Z}[G]$ frei ist, folgt aus der exakten Folge

$$0 = H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to$$
$$H_0(G, \mathbb{Z}[G]) \to H_0(G, \mathbb{Z}) \to 0$$

die Exaktheit der Folge

$$0 \longrightarrow H_1(G, \mathbb{Z}) \longrightarrow (I_G)_G \longrightarrow (\mathbb{Z}[G])_G \xrightarrow{\bar{\varepsilon}} \mathbb{Z} \longrightarrow 0$$

Nun gilt $(\mathbb{Z}[G])_G = \mathbb{Z}[G]/I_G\mathbb{Z}[G] = \mathbb{Z}[G]/I_G$ also ist $\bar{\varepsilon}$ ein Isomorphismus. Wir erhalten

$$H_1(G, \mathbb{Z}) \cong (I_G)_G = I_G/I_G^2$$

und nach 1.3 gilt $I_G/I_G^2 \cong G^{\mathrm{ab}}$. □

Lemma 1.12. *Für $G = \{1\}$ gilt*

$$H_i(\{1\}, A) = 0 \quad \forall\, i \geq 1.$$

Beweis. Für $G = \{1\}$ gilt $\mathbb{Z}[G] = \mathbb{Z}$. Daher: $H_i(\{1\}, A) = \mathrm{Tor}_i^{\mathbb{Z}}(A, \mathbb{Z}) = 0$ für $i \geq 1$, weil $\mathbb{Z}$ ein flacher $\mathbb{Z}$-Modul ist.

Alternativer Beweis: Für $G = \{1\}$ ist die Kategorie der G-Moduln gleich der Kategorie der abelschen Gruppen und $(-_G)$ ist der identische Funktor, also exakt $\Rightarrow\ L_i(-_G) = 0 \quad \forall\, i \geq 1$. □

1.4 Induzierte Moduln

Definition. Sei A ein G-Modul. Dann heißt $\mathrm{Ind}_G A = \mathbb{Z}[G] \otimes A$ der induzierte Modul zu A.

Bemerkung. $\mathrm{Ind}_G : G - \mathrm{Mod} \to G - \mathrm{Mod}$ ist ein exakter Funktor.

Definition. Ein G-Modul B heißt **induziert**, wenn es einen G-Modul A und einen Isomorphismus $B \cong \mathrm{Ind}_G A$ gibt.

Bezeichnung: Mit A^{tr} bezeichnen wir den G-Modul, der die gleiche unterliegende abelsche Gruppe hat wie A, aber triviale G-Wirkung.

Lemma 1.13. *Es gibt einen natürlichen Isomorphismus* $\mathrm{Ind}_G A^{\mathrm{tr}} \xrightarrow{\sim} \mathrm{Ind}_G A$.

Beweis. Als abelsche Gruppe gilt

$$\mathrm{Ind}_G A = \mathbb{Z}[G] \otimes A = \bigoplus_{g \in G} gA.$$

Daher setzt sich die Abbildung

$$g \otimes a \longmapsto g \otimes ga$$

zu einem Homomorphismus

$$\varphi\colon \mathbb{Z}[G] \otimes A^{\mathrm{tr}} \longrightarrow \mathbb{Z}[G] \otimes A$$

fort. Dies ist ein Isomorphismus, φ^{-1} ist gegeben durch $\varphi^{-1}(g \otimes a) = g \otimes g^{-1}a$. Nun gilt für $g, h \in G$, $a \in A^{\mathrm{tr}}$,

$$g\varphi(h \otimes a) = g(h \otimes ha) = gh \otimes gha = \varphi(gh \otimes a) = \varphi(g(\underbrace{h \otimes a}_{\in \mathbb{Z}[G] \otimes A^{\mathrm{tr}}})).$$

Daher ist φ ein Homomorphismus von G-Moduln. $\square$

Sei nun $U \subset G$ eine Untergruppe und sei A ein U-Modul.

Definition.

$$\mathrm{Ind}_G^U A = \mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} A.$$

Ind_G^U wird zum G-Modul durch $g(h \otimes_{\mathbb{Z}[U]} a) = gh \otimes_{\mathbb{Z}[U]} a$.

Bemerkung. Für den Spezialfall $U = \{1\}$ gibt uns 1.13 die natürliche Äquivalenz von Funktoren

$$\mathrm{Ind}_G \simeq \mathrm{Ind}_G^{\{1\}} \circ \mathrm{Res}_{\{1\}}^G \colon G - \mathrm{Mod} \longrightarrow G - \mathrm{Mod},$$

wobei $\mathrm{Res}_{\{1\}}^G \colon G - \mathrm{Mod} \to \{1\} - \mathrm{Mod} = \mathcal{A}b$ der Vergiss-Funktor ist.

Sei $S \subset G$ ein System von Vertretern der Linksnebenklassen G/U. Dann gilt als abelsche Gruppe

$$\begin{aligned}\mathrm{Ind}_G^U A &= \mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} A \\ &= \mathbb{Z}[U]^S \otimes_{\mathbb{Z}[U]} A \\ &= \bigoplus_{s\in S} s \cdot A.\end{aligned}$$

Sei OE $e \in S$. Dann identifizieren wir A mit der Untergruppe $e \cdot A \subseteq \mathrm{Ind}_G^U A$. Die G-Wirkung auf $\bigoplus_{s\in S} sA$ ist die folgende:

Für $g \in G$, $s \in S$ existieren eindeutig bestimmte $s_g \in S$, $u_g \in U$ mit $gs = s_g u_g$. Daher gilt

$$g(s \cdot a) = g \cdot s \cdot a = s_g \cdot u_g \cdot a.$$

Für $u \in U$ gilt daher $u \cdot e \cdot a = e \cdot ua$, d.h. A identifiziert sich mit $eA \subset \mathrm{Ind}_G^U A$ als U-Modul.

Ist nun B ein G-Modul und $\varphi : \mathrm{Ind}_G^U A \to B$ ein G-Homomorphismus, so ist $\varphi|_{eA} : A \to B$ ein U-Homomorphismus. Ist umgekehrt $\psi : A \to B$ ein U-Homomorphismus, so setze für $s \in S$

$$\psi(sa) = s\psi(a) \in B.$$

Wir erhalten so eine Ausdehnung von $\psi\colon eA \to B$ zu $\tilde{\psi}\colon \bigoplus_{s\in S} sA \to B$.

Für $g \in G$, $s \in S$, $a \in A$ gilt

$$\begin{aligned}\tilde{\psi}(gsa) &= \tilde{\psi}(s_g u_g a) = s_g \psi(u_g a) \\ &= s_g u_g \psi(a) \\ &= gs\psi(a) = g \cdot \tilde{\psi}(sa).\end{aligned}$$

Daher ist $\tilde{\psi}$ ein G-Homomorphismus

$$\tilde{\psi} : \mathrm{Ind}_G^U A \longrightarrow B.$$

$\tilde{\psi}$ ist der eindeutige G-Homomorphismus $\tilde{\psi}\colon \mathrm{Ind}_G^U A \to B$, der den U-Homomorphismus $\psi\colon eA \to B$ fortsetzt (gleiche Rechnung rückwärts).

Bezeichnen wir mit $\mathrm{Res}_U^G\colon G - \mathrm{Mod} \to U - \mathrm{Mod}$ den Vergiss-Funktor, so erhalten wir:

Satz 1.14 („Frobenius-Reziprozität“)**.** *Es gilt*

$$\mathrm{Ind}_G^U \dashv \mathrm{Res}_U^G.$$

Beide Funktoren sind exakt. Ind_G^U *überführt projektive U-Moduln in projektive G-Moduln und* Res_U^G *überführt injektive G-Moduln in injektive U-Moduln.*

Beweis. Die Adjunktion haben wir gerade bewiesen. Res_U^G ist offensichtlich exakt. $\mathrm{Ind}_G^U A = \mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} A$ und weil $\mathbb{Z}[G]$ ein freier $\mathbb{Z}[U]$-Modul ist (siehe 1.6) ist auch Ind_G^U exakt. Die verbleibenden Aussagen folgen aus **??**. □

Schließlich bemerken wir:

Lemma 1.15. *Sei G eine Gruppe und sei A ein induzierter G-Modul. Dann ist für jede Untergruppe $U \subset G$ der Modul $\mathrm{Res}_U^G A$ ein induzierter U-Modul.*

Beweis. Sei $A = \mathrm{Ind}_G B$ und nach 1.13 sei ohne Einschränkung B ein trivialer G-Modul. Dann gilt

$$\begin{array}{rcl} A & = & \mathbb{Z}[G] \otimes_{\mathbb{Z}} B \\ & = & \mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} \mathbb{Z}[U] \otimes_{\mathbb{Z}} B \\ (\text{als } U - \text{Modul}) & \cong & \mathbb{Z}[U]^{(S)} \otimes_{\mathbb{Z}[U]} \mathbb{Z}[U] \otimes_{\mathbb{Z}} B \\ & \cong & \mathbb{Z}[U]^{(S)} \otimes_{\mathbb{Z}} B \\ & \cong & (\mathbb{Z}[U] \otimes_{\mathbb{Z}} B)^{(S)} \\ & = & \mathbb{Z}[U] \otimes_{\mathbb{Z}} B^{(S)} \end{array}$$

wobei S ein Repräsentantensystem von G/U ist. □

1.5 Homologisch triviale Moduln

Im folgenden lassen wir die Bezeichnung Res_U^G weg und fassen, wenn nötig, A als U-Modul auf.

Definition. Ein G-Modul M heißt **homologisch trivial**, wenn $H_n(U, M) = 0$ für alle $n \geq 1$ und jede Untergruppe $U \subset G$.

Bemerkung. Projektive Moduln sind homologisch trivial: (Nach 1.6 ist M auch projektiver U-Modul für jedes $U \subset G$).

Satz 1.16. *Induzierte Moduln sind homologisch trivial.*

Beweis. Nach 1.15 und 1.13 g.z.z.: $H_n(G, \mathrm{Ind}_G A) = 0$ für alle $n \geq 1$ und jeden trivialen G-Modul A. Nun gilt:

$$H_n(G, \mathrm{Ind}_G A) = H_n(G, \mathbb{Z}[G] \otimes_{\mathbb{Z}} A)$$
$$= H_n(P_\bullet \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] \otimes_{\mathbb{Z}} A) = H_n(P_\bullet \otimes_{\mathbb{Z}} A)$$

wobei $P_\bullet \to \mathbb{Z}$ eine beliebige projektive Auflösung von $\mathbb{Z}$ als G-Modul ist. Nach 1.6 ist $P_\bullet \to \mathbb{Z}$ insbesondere eine projektive Auflösung in $\mathcal{A}b$. Daher gilt für $n \geq 1$:

$$\begin{array}{rcl} H_n(P_\bullet \otimes_{\mathbb{Z}} A) & = & \mathrm{Tor}_n^{\mathbb{Z}}(\mathbb{Z}, A) \\ & = & 0. \end{array}$$

□

Sei nun A ein G-Modul. Tensoriert man die Augmentation $\varepsilon\colon \mathbb{Z}[G] \to \mathbb{Z}$ mit A erhält man eine exakte Folge

$$0 \longrightarrow A_1 \longrightarrow \mathrm{Ind}_G A \longrightarrow A \longrightarrow 0.$$

Setzt man mit $\mathrm{Ind}_G A_1 \to A_1$ fort, so erhält man induktiv eine natürliche Auflösung von A durch homologisch triviale Moduln.

Dieses Vorgehen läßt sich verallgemeinern.

Satz 1.17 (Shapiro-Lemma)**.** *Sei $U \subset G$ eine Untergruppe und A ein U-Modul. Dann gilt*

$$H_n(U, A) \cong H_n(G, \mathrm{Ind}_G^U A)$$

für alle $n \geq 0$.

Beweis. Sei $P \to \mathbb{Z}$ eine Auflösung durch projektive G-Moduln. Dann gilt

$$\begin{aligned} H_n(G, \mathrm{Ind}_G^U A) &= H_n(P_\bullet \otimes_{\mathbb{Z}[G]} \mathrm{Ind}_G^U A) \\ &= H_n(P_\bullet \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} A) \\ &= H_n(P_\bullet \otimes_{\mathbb{Z}[U]} A) \\ &= H_n(U, A) \end{aligned}$$

weil $P_\bullet \to \mathbb{Z}$ auch eine Auflösung durch projektive U-Moduln ist. □

1.6 Restriktion und Korestriktion

Sei $U \subset G$ eine Untergruppe und A ein G-Modul. Wir konstruieren eine natürliche Abbildung $cor_G^U\colon H_n(U, A) \to H_n(G, A)$ für alle $n \geq 0$.

Sei M ein G-Modul. Dann haben wir eine natürliche Abbildung $M_U \xrightarrow{\text{kan}} M_G$. Ist nun $P_\bullet \to \mathbb{Z}$ eine G-projektive Auflösung, so erhalten wir (setze $M = P_i \otimes A$) eine Abbildung

$$(P_\bullet \otimes A)_U \longrightarrow (P_\bullet \otimes A)_G$$

Definition. Die auf der Homologie induzierte Abbildung

$$cor_G^U\colon H_n(U, A) \longrightarrow H_n(G, A)$$

heißt die **Korestriktion(sabbildung)**.

Beispiel. $A = \mathbb{Z}$, $n = 1$.

$$cor_G^U\colon U^{\mathrm{ab}} = H_1(U, \mathbb{Z}) \longrightarrow H_1(G, \mathbb{Z}) = G^{\mathrm{ab}}$$

ist die natürliche, durch $U \hookrightarrow G$ induzierte Abbildung auf den Abelisierungen.

Nun nehmen wir an, dass $(G : U) < \infty$ gilt. Für jeden G-Modul M haben wir die „Norm-Abbildung“

$$M_G \longrightarrow M_U \quad , \quad m \longmapsto \sum_{s \in U \backslash G} sm.$$

Diese ist wohldefiniert, denn für $u \in U$ gilt $usm - sm = (u-1)(sm) \in I_U M$, d.h. wir erhalten $M \xrightarrow{N} M_U$. Für $g \in G$, $m \in M$ gilt

$$\begin{aligned} N((g-1)m) &= \sum_{s \in U \backslash G} sgm - sm \\ &= \sum_{s \in U \backslash G} sgm - \sum_{s \in U \backslash G} sm. \end{aligned}$$

Nun ist die Multiplikation von rechts mit g eine Bijektion $U \backslash G \to U \backslash G$, also gilt $N((g-1)m) = 0$. Wir erhalten $N : M_G = M/I_G M \to M_U$. Angewendet auf eine projektive Auflösung $P_\bullet \otimes A$ erhalten wir eine Abbildung

$$(P_\bullet \otimes A)_G \longrightarrow (P_\bullet \otimes A)_U.$$

Definition. Die auf der Homologie induzierte Abbildung $res_U^G \colon H_n(G, A) \to H_n(U, A)$ heißt die **Restriktion**.

Beispiel. Für $(G \colon U) < \infty$, $n = 1$, $A = \mathbb{Z}$, erhalten wir einen (mysteriösen) Homomorphismus

$$\mathrm{Ver} \colon G^{\mathrm{ab}} \longrightarrow U^{\mathrm{ab}}.$$

Dieser heißt **Verlagerung**.

Ein der für die Zahlentheorie wichtiger gruppentheoretischer Satz ist der

Satz 1.18 (Hauptidealsatz)**.** *Sei G eine endlich erzeugte Gruppe und wir nehmen an, dass die Kommutatorgruppe $H = [G, G] \subset G$ endlichen Index hat. Dann ist die Verlagerung*

$$\mathrm{Ver} : G^{\mathrm{ab}} \longrightarrow H^{\mathrm{ab}}$$

die Nullabbildung.

Beweis. Siehe Neukirch: „Zahlentheorie“. □

Zurück zur alten Situation $(G \colon U) = n < \infty$. Die Komposition der konstruierten Abbildungen

$$M_G \xrightarrow{N} M_U \xrightarrow{\mathrm{kan}} M_G$$

ist die Multiplikation mit n, denn

$$\sum_{s \in U \backslash G} sm - n \cdot m = \sum_{s \in U \backslash G} (s-1)m \in I_G M.$$

Wir wenden das auf $P_\bullet \otimes A$ an und erhalten:

Satz 1.19. *Für* $(G\colon U) = n < \infty$ *gilt* $cor_G^U \circ res_U^G = n \cdot \mathrm{id}$.

Korollar 1.20. *Sei G eine endliche Gruppe der Ordnung n und sei A ein G-Modul, so dass die n-Multiplikation $A \xrightarrow{\cdot n} A$ ein Isomorphismus ist. Dann gilt*

$$H_i(G, A) = 0 \quad \forall\, i \geq 1.$$

Beweis. Nach 1.19 sind die Selbstabbildungen $cor_G^{\{1\}} res_{\{1\}}^G$ und $\cdot n$ von $H_i(G, A)$ dieselben. Nach Voraussetzung ist $\cdot n$ ein Isomorphismus und wegen $H_i(\{1\}, A) = 0$ für $i \geq 1$ ist $cor \circ res$ die Nullabbildung. Die Nullabbildung ist aber nur auf der trivialen Gruppe ein Isomorphismus. □

Korollar 1.21. (i) *Sei G eine endliche Gruppe und A ein G-Modul der als abelsche Gruppe eindeutig teilbar ist. Dann gilt $H_i(G, A) = 0 \quad \forall\, i \geq 1$.*

(ii) *Sei G eine endliche Gruppe und sei A ein endlicher G-Modul. Gilt $(\#G, \#A) = 1$, so folgt*

$$H_i(G, A) = 0$$

für alle $i \geq 1$.