Algebra 1 (basics) – Overview

1. Grundlagen

- Definition ‘Halbgruppe’; ‘neutrales Element’; ‘Monoid’; ‘inverses Element’; ‘Gruppe’, ‘kommutativ/ Abelsch’
- $(\mathbb{N}_0,+)$ ist Monoid.
- $(\mathbb{Z}/n\mathbb{Z};+)$ ist Gruppe.
- $(\mathbb{Z}/n\mathbb{Z};+)$ heißt die zyklische Gruppe der Ordnung n.
- Definition ‘$\mathrm{Abb}(M,M)$’: $\mathrm{Abb}(M,M) := \{f : M \to M \text{ Abbildung}\}$; ‘$\mathrm{Bij}(M,M)$’: $\mathrm{Bij}(M,M) := \{f : M \to M \text{ Bijektion}\}$
- einfache Eigenschaften von Gruppen:
  - Das neutrale Element e ist eindeutig bestimmt.
  - Zu jedem a ist das inverse Element a^{-1} eindeutig besimmt.
  - $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$
  - Kürzungregeln:
    - $a \circ b = a \circ c \Rightarrow b = c$
    - $b \circ a = c \circ a \Rightarrow b = c$
  - Die Rechtstranslation $\rho_a : \begin{matrix} G \to G \\ b \mapsto b \circ a \end{matrix}$ und die Linkstranslation $\lambda_a : \begin{matrix} G \to G \\ b \mapsto a \circ b \end{matrix}$ sind bijektiv.
- Darstellung endlicher Gruppen via Gruppentafel
- Definition ‘Untergruppe $U \subseteq G$’: $a,b \in U \Rightarrow a \circ b \in U \wedge a \in U \Rightarrow a^{-1} \in U$; ‘Homomorphismus von Gruppen $f : G \to H$’: $f(a \circ b) = f(a) * f(b)$; ‘Isomorphismus $f : G \to H$’: bijektiver Homomorphismus von Gruppen; ‘G und H sind isomorph’: Es gibt einen Isomorphismus $f : G \to H$.; ‘Automorphismus’: ein Isomorphismus $f : G \to G$; ‘triviale Untergruppe’: $(\{e\},\circ)$
- $(\mathbb{R},+)$ und $(\mathbb{R}_+,\cdot)$ sind isomorph.
  - Beweis: $\exp : \begin{matrix} \mathbb{R} \to \mathbb{R}_+ \\ x \mapsto \underbrace{e}_{\text{Euler's Zahl}}{}^{x} \end{matrix}$ ist der gesuchte Isomorphismus, denn $\exp(x+y) = e^{x+y} = e^x \cdot e^y = \exp(x) \cdot \exp(y)$.
- Eigenschaften von Untergruppen und Homomorphismen von Gruppen:
  - $f(e_G) = e_H$
  - $U \subseteq G$ Untergruppe $\Rightarrow f(U) \subseteq H$ Untergruppe
  - $V \subseteq H$ Untergruppe $\Rightarrow f^{-1}(V) \subseteq G$ Untergruppe
  - $(f(a))^{-1} = f(a^{-1})$
  - f injektiv $\Leftrightarrow \ker(f) = \{e_G\}$, wobei $\ker(f) = f^{-1}(\{e_H\})$
  - $f : G \to H$ Isomorphismus $\Rightarrow f^{-1} : H \to G$ Isomorphismus
- Definition ‘n-te symmetrische Gruppe/ n-te Permutationgruppe S_n’: $S_n := \mathrm{Bij}(\{1,\ldots,n\} \to \{1,\ldots,n\})$; ‘Permutationen’: die Elemente von S_n
- $\# S_n = n!$

- S_n ist für $n \geq 3$ ist nicht kommutativ.
- Defnition 'Transposition': Permutation, die nur genau 2 Elemente vertauscht
- Jede Permutation lässt sich als Komposition von Transpositionen darstellen (allerdings nicht eindeutig).
- Definition 'gerade Permutation': Die Permutation lässt sich als Komposition von gerade vielen Transpositionen darstellen.; 'ungerade Permutation': analog; 'Signum einer Permutation $\text{sign}: \begin{matrix} S_n \to \{-1,1\} \\ \sigma \mapsto \begin{cases} -1, \text{falls } \sigma \text{ ungerade} \\ 1, \text{falls } \sigma \text{ gerade} \end{cases} \end{matrix}$; '$n$-te alternierende Gruppe A_n': $A_n := \ker(\text{sign}) \subseteq S_n$
- Definition 'Ordnung von $a \in G$ $\text{ord}_G(a)$': $\text{ord}_G(a) = \begin{cases} \min\{i > 0 \mid a^i = e\}, \text{falls dies existiert} \\ \infty \text{ sonst} \end{cases}$;
  'Ordnung einer endlichen Gruppe G $\text{ord}(G)$': $\text{ord}(G) := \#G$
- kleiner Fermat's Satz: G endliche Gruppe, dann:
  - $U := \{e, a, a^2, \ldots\} = \{e, a, a^2, \ldots, a^{\text{ord}_G(a)-1}\} =: \langle a \rangle$ ist kommutative Untergruppe von G,
    - Beweis: $a^i \circ a^j = a^{i+j} \in U$ und $(a^i)^{-1} = a^{\text{ord}_G(a)-i}$
  - $\text{ord}_G(a) \mid \text{ord}(G)$
    - Beweis:
      - $G = \dot{\bigcup_{i=1}^{s}} b_i \underbrace{U}_{:=\langle a \rangle}$ für gewisse b_i, weil:

        $b_i U \cap b_j U \neq \{\} \Rightarrow \exists a^k, a^l \in U : b_i a^k = b_j a^l \Rightarrow b_i = b_j \underbrace{a^{l-k}}_{\in U} \Rightarrow b_i \in b_j U$

        $\Rightarrow b_i U \subseteq b_j U U = b_j U$
      - Weil λ_{b_i} bijektiv ist, ist $\# b_i U = \# U = \text{ord}_G(a)$.
      - daher: $\#G = s \cdot \text{ord}_G(a)$
- Definition '$\mathbb{F}_p^*$' (p Primzahl): $\mathbb{F}_p^* := (\mathbb{Z}/p\mathbb{Z}) \setminus \{\overline{0}\}$; 'primitive Restklasse modulo p $a + p\mathbb{Z} \in (\mathbb{F}_p^*, \cdot)$': $a + p\mathbb{Z}$ erzeugt $(\mathbb{F}_p^*, \cdot)$
- $a + p\mathbb{Z}$ erzeugt $(\mathbb{F}_p^*, \cdot) \Leftrightarrow \text{ord}_{\mathbb{F}_p^*}(a + p\mathbb{Z}) = p - 1$
- Definition 'zyklische Gruppe G': $\exists a \in G : G = \{a^i\}$; 'primitives/ erzeugendes Element a von G': $G = \{a^i\}$; '$G = \langle a \rangle$': $G = \{a^i\}$
- Zyklische Gruppen sind kommutativ.
- Eigenschaften zyklischer Gruppen: G zyklische Gruppe mit primitivem Element a.
  - $\text{ord}_G(a) = \infty \Rightarrow \varphi : \begin{matrix} \mathbb{Z} \to G \\ i \mapsto a^i \end{matrix}$ ist ein Isomorphismus von Gruppen.
    - Beweis: φ ist Homomorphismus von Gruppen, surjektiv (nach Definition) und injektiv, weil $\ker(\varphi) = \{i \in \mathbb{Z} \mid \varphi(i) = e_G\} = \{0\}$ (wegen $\text{ord}_G(a) = \infty$)
  - $n := \text{ord}_G(a) < \infty \Rightarrow \psi : \begin{matrix} \mathbb{Z}/n\mathbb{Z} \to \mathrm{G} \\ i + n\mathbb{Z} \mapsto a^i \end{matrix}$ ist ein Isomorphismus von Gruppen.
    - Beweis: ψ ist offensichtlich Homomorphismus von Gruppen und bijektiv.
  - $U \subseteq G \wedge n := \text{ord}(G) < \infty \Rightarrow U \cong \{0 + n\mathrm{U}, m + n\mathbb{Z}, 2m + n\mathbb{Z}, \ldots\}$

- Beweisidee: $\{0+n\mathbb{U}, m+n\mathbb{Z}, 2m+n\mathbb{Z}, \ldots\} \hat{=} \left\{e, a^m, \underbrace{\left(a^m\right)^2}_{=a^{2m}}, \ldots\right\}$

- G zyklisch $\Rightarrow U \subseteq G$ zyklisch
- $n := \mathrm{ord}(G) < \infty \Rightarrow \left(b := \psi(m+n\mathbb{Z}) = a^m \text{ ist primitives Element von } G. \Leftrightarrow \mathrm{ggT}(m,n) = 1\right)$
  - Beweisidee: $\mathrm{ggT}(m,n) = 1 \Leftrightarrow \mathrm{kgV}(m,n) = mn \Rightarrow$ Erst $mn \in \mathbb{Z}/n\mathbb{Z}$ ist wieder gleich $\overline{0}$, d. h. erst $a^{mn} = \left(a^m\right)^n = e_G$, d. h. $\mathrm{ord}_G\left(a^m\right) = n$, d. h. $G = \left\langle a^m \right\rangle$.
- $n := \mathrm{ord}(G) < \infty \Rightarrow G$ besitzt genau $\underbrace{\varphi(n) := \#\{0 < m < n \mid \mathrm{ggT}(m,n) = 1\}}_{\text{Euler's φ-Funktion}}$ primitive Elemente.
  - Beweis: Folgt aus ‘$n := \mathrm{ord}(G) < \infty \Rightarrow \left(b := \psi(m+n\mathbb{Z}) = a^m \text{ ist primitives Element von } G. \Leftrightarrow \mathrm{ggT}(m,n) = 1\right)$’.
- $n := \mathrm{ord}(G) < \infty \wedge m \in \mathbb{Z} : \mathrm{ggT}(m,n) = 1 \Rightarrow \mathrm{ord}_G\left(a^m\right) = \mathrm{ord}_G(a) = n$
  - Beweis: Folgt aus ‘$n := \mathrm{ord}(G) < \infty \Rightarrow \left(b := \psi(m+n\mathbb{Z}) = a^m \text{ ist primitives Element von } G. \Leftrightarrow \mathrm{ggT}(m,n) = 1\right)$’.

2. Kristallographie

- left out

3. Restklassengruppen

3.1 Operationen von Gruppen auf Mengen

- Definition ‘Operation von G auf M’ (M Menge): $\alpha : \begin{matrix} G \times M \to M \\ (g,m) \mapsto g(m) \end{matrix}$ mit:
  - $e(m) = m$
  - $(g_2 \circ g_1)(m) = g_2(g_1(m))$
- Definition ‘treue Operation’: $g_1(m) = g_2(m) \forall m \in M \Rightarrow g_1 = g_2$, d. h. injektiv
- Definition ‘Operation auf sich durch Linkstranslation’: $\lambda : \begin{matrix} G \times G \to G \\ (g_1,g_2) \mapsto g_1 \circ g_2 \end{matrix}$; ‘Operation auf sich durch Rechtstranslation’: $\rho : \begin{matrix} G \times G \to G \\ (g_1,g_2) \mapsto g_2 \circ g_1^{-1} \end{matrix}$; ‘Operation auf sich durch Konjugation’: $\kappa : \begin{matrix} G \times G \to G \\ (g_1,g_2) \mapsto g_1 \circ g_2 \circ g_1^{-1} \end{matrix}$; ‘Operation von G auf der Menge der Untergruppen von G U durch Konjugation’: $\overline{\kappa} : \begin{matrix} G \times U \to U \\ \left(g_1, \underbrace{u}_{\text{Untergruppe}}\right) \mapsto g_1 \circ u \circ g_1^{-1} \end{matrix}$
- Definition ‘Isotropiegruppe von $N \subseteq M$ G_N’ ($\alpha : G \times M \to M$):

$G_N := \{g \in G | g(n) = n \forall n \in N\}$; 'Fixpunkt von α m': $g(m) = m \forall g \in G$; 'Bahn von m unter α Gm': $Gm := \{g(m)\}$; 'transitive Operation α': $\forall m_1, m_2 \in M \exists g : m_2 = g(m_1)$

- α ist transitiv. $\Leftrightarrow$ Es existiert nur eine Bahn, nämlich $Gm = M \forall m$.
  - Beweis:
    - '$\Rightarrow$':
      - Wähle m_1 beliebig und durchlaufe mit m_2 ganz M. Nach Voraussetzung gibt es für alle m_2 ein g mit $m_2 = g(m_1)$, also $Gm_1 = M$.
      - Da dies unabhängig von m_1 war, gilt $Gm = M \forall m$. Also existiert nur eine Bahn.
    - '$\Leftarrow$':
      - Wähle m_1 beliebig. Es gilt $Gm_1 = M$.
      - Das bedeutet, dass jedes $m_2 \in M$ als ein Funktionswert für ein g vorkommt, d. h. $\forall m_2 \exists g : m_2 = g(m_1)$.
      - Das dies für alle m_1 gilt, gilt $\forall m_1, m_2 \exists g : m_2 = g(m_1)$
- Definition 'Zentralisator von $\underbrace{H}_{\text{nur Teilmenge nötig}} \subseteq G$ G_H': die Isotropiegruppe $G_H := \left\{ g \in G \middle| \underbrace{gh = hg}_{\text{bzw. } ghg^{-1} = h} \forall h \in H \right\}$; 'Zentrum von G $Z(G)$': $Z(G) := G_G = \left\{ g \in G \middle| \underbrace{gh = hg}_{\text{bzw. } ghg^{-1} = h} \forall h \in G \right\}$; 'Normalisator von $\underbrace{u}_{\in U, \text{d.h. } u \text{ Untergruppe}} \subseteq G$': die Isotropiegruppe $G_{\{u\}} = \{g \in G | gug^{-1} = u\}$; 'Konjugationsklasse von h': die Bahn $Gh = \{ghg^{-1}\}$; 'Konjugationsklasse von $\underbrace{u}_{\in U, \text{d.h. } u \text{ Untergruppe}} \subseteq G$': die Bahn $Gu = \{gug^{-1}\}$
- $\alpha : G \times M \to M$ Operation, dann:
  - M ist die disjunkte Vereinigung der Bahnen.
    - Beweis:
      - Zeige $Gm_1 \cap Gm_2 = \{\}$ xor $Gm_1 = Gm_2$.
      - Sei $m \in Gm_1 \cap Gm_2$, dann $m = \underbrace{g_1(m_1)}_{\in Gm_1} = \underbrace{g_2(m_2)}_{\in Gm_2}$.
      - Dann gilt für alle $h \in G$ $\underbrace{h(m_1)}_{\in Gm_1} = (h \circ g_1^{-1} \circ g_1)(m_1) = (h \circ g_1^{-1})(g_1(m_1)) = (h \circ g_1^{-1})(g_2(m_2)) = \underbrace{(h \circ g_1^{-1} \circ g_2)(m_2)}_{\in Gm_2}$.
      - Also $Gm_1 \subseteq Gm_2$.
      - analog $Gm_1 \supseteq Gm_2$, also $Gm_1 = Gm_2$
  - G endlich, dann: $\#G = \#(Gm) \cdot \#\left(\underbrace{G_{\{m\}}}_{=\{g \in G | g(m) = m\}} \right)$
    - Beweis:
      - Sei $Gm = \{g_1(m), \ldots, g_r(m)\}$ und $G_{\{m\}} = \{h_1, \ldots, h_s\}$.
      - Es gibt mindestens rs verschiedene Elemente, denn die Produkte $g_i h_j$ sind alle unterschiedlich:

$g_i \circ h_j = g_k \circ h_l \Rightarrow g_i(m) = g_i(h_j(m)) = (g_i \circ h_j)(m) = (g_k \circ h_l)(m) = g_k(h_l(m))$
$= g_k(m) \Rightarrow g_i = g_k$

- Es folgt weiter: $g_i \circ h_j = g_k \circ h_l \Rightarrow g_i \circ h_j = g_i \circ h_l \Rightarrow h_j = h_l$
- insgesamt: $g_i \circ h_j = g_k \circ h_l \Leftrightarrow (i,j) = (k,l)$
- also: $\#G \geq rs$
- Andererseits lässt sich jedes $g \in G$ darstellen als $g = g_i h_j$ für ein paar (i,j), denn:
- Zu jedem g gibt es wegen $Gm = \{g_1(m),\ldots,g_r(m)\}$ ein g_i mit $g(m) = g_i(m)$.
- Wegen $g_i^{-1}(g(m)) = g_i^{-1}(g_i(m)) = m$ ist $g_i^{-1} \circ g \in G_{\{m\}}$, also $g_i^{-1} \circ g = h_j$ für ein h_j.
- Also $g = g_i \circ h_j$ und somit $\#G \leq rs$
- insgesamt: $\#G = rs$

- Definition 'Rechtsnebenklasse von g bzgl. $u \in U$': die Bahn $ug = \{vg | v \in u\}$; 'Linksnebenklasse von g bzgl. $u \in U$': die Bahn $gu = \{gv | v \in u\}$; 'G/u': Menge der Linksnebenklassen von Elementen von G bzgl. u, $G/u = \{gu | g \in G\}$; 'Index von u in G $[G:U]$': $[G:U] := \begin{cases} \#(G/u), \text{falls } \#(G/u) < \infty \\ \infty \text{ sonst} \end{cases}$
- Satz von Lagrange: $\#G = [G:u] \cdot (\#u)$
  - Beweis: analog zum Beweis von '$\#G = \#(Gm) \cdot \#(G_{\{m\}})$', wobei $G/u = \{g_1 u,\ldots,g_r u\}$ die Rolle von Gm übernimmt und $u = \{u_1,\ldots,u_s\}$ die Rolle von $G_{\{m\}}$
- Klassengleichung: G operiere auf sich durch Konjugation und $g_1,\ldots,g_r \in G : G = \dot{\bigcup_{i=1}^{r}} Gg_i$, dann: $\#G = \sum_{i=1}^{r} [G:Z(g_i)] = \#Z(G) + \sum_{\{i | [G:Z(g_i)] > 1\}} [G:Z(g_i)]$

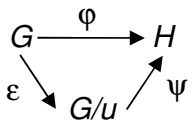
3.2 Normalteiler

$(gu) \cdot (hu) = (gh)u$

- $\Leftrightarrow gu = ug$
- $\Leftrightarrow gug^{-1} = u$
- $\Leftrightarrow gug^{-1} \subseteq u$

- Definition 'Normalteiler von G u': Die Untergruppe u erfüllt die gerade genannten Bedingungen.; '$u \lhd G$': u ist Normalteiler von G.
- G kommutativ $\Rightarrow$ Jede Untergruppe u ist Normalteiler.
  - Beweis: $gu = ug \forall g \in G$
- $f : G \to H$ Homomorphismus von Gruppen $\Rightarrow \ker(f) \lhd G$
  - Beweis:
    - Zeige $g \circ \ker(f) \circ g^{-1} \subseteq \ker(f)$. Sei $g' \in \ker(f)$. Mit anderen Worten: $f(g') = e_H$
    - $f(g \circ g' \circ g^{-1}) = f(g) * f(g') * f(g^{-1}) = f(g) * e_H * f(g^{-1}) = f(g) * f(g^{-1}) = f(g) * (f(g))^{-1} = e_H$
- $A_n \lhd S_n$
  - Beweis: $\text{sign}(A_n) = 1$, somit $\text{sign}(\sigma A_n \sigma^{-1}) = 1 \forall \sigma \in S_n \Rightarrow \sigma A_n \sigma^{-1} \in A_n$. Alternativ: $A_n = \ker(\text{sign})$.

- $u \lhd G \Rightarrow (G/u, \circ)$ mit $\circ : \begin{matrix} G/u \times G/u \to G/u \\ (gu, hu) \mapsto (gh)u \end{matrix}$ ist Gruppe. (D. h. teilt man einen Normalteiler aus der Gruppe heraus, so erhält man eine Restklassengruppe.)
  - Beweis:
    - Assoziativität:
      $(g_1u \cdot g_2u) \cdot g_3u = (g_1g_2u) \cdot g_3u = (g_1g_2)g_3u = g_1(g_2g_3)u = g_1u \cdot (g_2g_3u)$
      $= g_1u \cdot (g_2u \cdot g_3u)$
    - neutrales Element: eu
    - inverses Element: $g^{-1}u$
- Definition 'Restklassengruppe': $(G/u, \circ)$; 'kanonischer Epimorphismus auf die Restklassengruppe ε': der surjektive Homomorphismus von Gruppen $\varepsilon : \begin{matrix} G \to G/u \\ g \mapsto gu \end{matrix}$
- universelle Eigenschaft der Restklassengruppe: Seien $\varphi : G \to H$ ein Homomorphismus von Gruppen, $u \lhd G$ und $u \subseteq \ker(\varphi)$. Es gibt einen eindeutig bestimmten Homomorphismus von Gruppen $\psi : G/u \to H$, so dass dieses Diagramm kommutiert:



  - Beweis:
    - definiere: $\psi(gu) := \varphi(g)$
    - Problem: Durch das modulo-Rechnen geht Information verloren, da mehrere Elemente aus G auf dassselbe Element in G/u abgebildet werden. Werden diese dann mittels ψ nach H abgebildet, könnte es also passieren, dass 2 verschiedene Elemente aus G, wenn sie mit φ abgebildet werden, auch auf 2 verschiedene Elemente aus H abgebildet werden. Wenn die beiden Elemente aus G jetzt aber in derselben Restklasse modulo u liegen, dann würden sie durch ε auf dassselbe Element in G/u abgebildet werden (Informationsverlust) und könnten durch ψ dann nicht wieder auf verschiedene Elemente in H abgebildet werden.
    - Zeige, dass Elemente von G, die modulo u in derselben Restklasse liegen (also $g_1u = g_2u$), durch φ tatsächlich auch auf dasselbe Element in H abgebildet werden (also $\varphi(g_1) = \varphi(g_2)$), was von vornherein nicht klar ist.:

$$g_1u = g_2u \underbrace{\Leftrightarrow}_{\text{Definition von } gu} \{g_1u_i \mid u_i \in U\} = \{g_2u_j \mid u_j \in U\} \Rightarrow \exists u_1, u_2 \in u : g_1u_1 = g_2u_2$$

$$\Rightarrow \underbrace{g_2^{-1}g_1 = u_2u_1^{-1} \in u}_{\substack{\text{vergleiche mit dem Üblichen:} \\ \bar{a}=\bar{b} \Leftrightarrow a-b \in U \Leftrightarrow -b+a \in U}} \underbrace{\Rightarrow}_{\text{wegen } u \subseteq \ker(\varphi)} g_2^{-1}g_1 \in \ker(\varphi) \Rightarrow \varphi(g_2^{-1}g_1) = e_H \Rightarrow \varphi(g_2^{-1}) * \varphi(g_1) = e_H$$

$$\Rightarrow \varphi(g_1) = \varphi(g_2)$$

3.3 Noether's Isomorphiesätze

- der Homomorphiesatz für Gruppen: $\varphi : G \to H$ surjektiver Homomorphismus von Gruppen, dann induziert φ einen Isomorphismus von Gruppen $\overline{\varphi} : \begin{matrix} G/\ker(\varphi) \to H \\ g\ker(\varphi) \mapsto \varphi(g) \end{matrix}$
  - Beweis:
    - Homomorphismus: Folgt aus der universellen Eigenschaft der Restklassengruppe,

weil $\ker(\varphi) \lhd G$; wähle $\overline{\varphi} := \psi$.

- surjektiv: Weil $\varphi = \overline{\varphi} \circ \varepsilon$ surjektiv ist.
- injektiv: $\overline{\varphi}(g\ker(\varphi)) = e_H \Rightarrow \varphi(g) = e_H \Rightarrow g \in \ker(\varphi) \Rightarrow g\ker(\varphi) = \underbrace{\ker(\varphi)}_{\text{Nullelement von } G/\ker(\varphi)}$

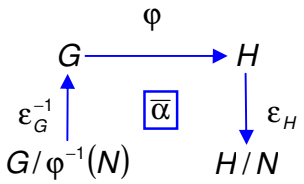
- Normalteiler und Homomorphismus von Gruppen:
  - $U \lhd G \wedge \varphi$ surjektiv $\Rightarrow \varphi(U) \lhd H$:
    - Beweis:
      - $\forall h \in H \exists g \in G : h = \varphi(g)$, weil φ surjektiv

        $h * \varphi(U) * h^{-1} = \varphi(g) * \varphi(U) * (\varphi(g))^{-1} = \varphi(g) * \varphi(U) * \varphi(g^{-1}) = \varphi(gUg^{-1}) \underbrace{=}_{\text{weil } U \lhd G} \varphi(U)$

        $\Leftrightarrow \varphi(U) \lhd H$
  - $V \lhd H \Rightarrow \varphi^{-1}(V) \lhd G$:
    - Beweis: Sei $g' \in \varphi^{-1}(V)$.

      $\varphi(g \circ g' \circ g^{-1}) = \varphi(g) * \varphi(g') * \varphi(g^{-1}) \in \varphi(g) * V * \varphi(g^{-1}) \underbrace{=}_{\text{wegen } V \lhd H} V$

      $\Leftrightarrow \varphi^{-1}(\varphi(g) * V * \varphi(g^{-1})) = \varphi^{-1}(V) \Leftrightarrow g \circ \varphi^{-1}(V) \circ g^{-1} = \varphi^{-1}(V) \Leftrightarrow \varphi^{-1}(V) \lhd G$
  - φ surjektiv $\Rightarrow$ φ ist Bijektion zwischen $\{U \lhd G \mid U \supseteq \ker(\varphi)\}$ und $\{V \lhd H\}$
    - Beweis: Folgt aus eben Gezeigtem.
- $N \lhd H$, dann: $\alpha : G \xrightarrow{\varphi} H \xrightarrow{\varepsilon_H} H/N$ liefert einen injektiven Homomorphismus von Gruppen $\overline{\alpha} : G/\varphi^{-1}(N) \to H/N$. Ist φ surjektiv, so ist $\overline{\alpha}$ ein Isomorphismus von Gruppen.



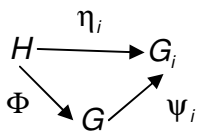
- $N \lhd G$, U Untergruppe, dann: UN ist Untergruppe von G und $N \lhd UN$ und $N \cap U \lhd U$
- 1. Noether's Isomorphiesatz: $N \lhd G$, U Untergruppe, dann: Durch $\varphi : \begin{matrix} U \to G/N \\ u \mapsto uN \end{matrix}$ wird ein Isomorphismus von Gruppen $\overline{\varphi} : U/N \cap U \xrightarrow{\sim} UN/N$ induziert.
  - Beweisidee: Verwende in diesem Abschnitt Gezeigtes.
- 2. Noether's Isomorphiesatz: $N_1, N_2 \lhd G$ mit $N_2 \subseteq N_1$, dann: $\psi : G \xrightarrow{\alpha} G/N_2 \to (G/N_2)/(N_1/N_2)$ induziert einen Isomorphismus von Gruppen $\overline{\psi} : G/N_1 \xrightarrow{\sim} (G/N_2)/(N_1/N_2)$
  - Beweisidee: Verwende in diesem Abschnitt Gezeigtes.

4. Konstruktion von Gruppen

4.1 Produkte

- Definition 'direktes Produkt $\prod_{i=1}^{n} G_i$': $\prod_{i=1}^{n} G_i := G_1 \times \ldots \times G_n$ ($n = \infty$ zulässig)

- $G := \prod_{i=1}^{n} G_i$, $\circ : \left(\begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix}, \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} \right) \overset{G \times G \to G}{\mapsto} \begin{pmatrix} g_1 h_1 \\ \vdots \\ g_n h_n \end{pmatrix}$, dann: $(G, \circ)$ ist Gruppe.
  - Beweis: Klar, denn in jeder Komponente wird die Gruppenstruktur der entsprechenden Gruppe ausgenutzt.
- $\varphi_j : g_j \overset{G_j \to G}{\mapsto} \begin{pmatrix} e_{G_1} \\ \vdots \\ e_{G_{j-1}} \\ g_j \\ e_{G_{j+1}} \\ \vdots \\ e_{G_n} \end{pmatrix}$ ist injektiver Homomorphismus von Gruppen.
  - Beweis: Klar, denn dies ist die normale Einbettung.
- $\varphi_j(G_j) \cong G_j \wedge \varphi_j(G_j) \lhd G$:
  - Beweis:
    - $\varphi_j(G_j) \cong G_j$ ist klar.
    - $\varphi_j(G_j) \lhd G$, weil: $\vec{g} \circ \varphi_j(g') \circ \vec{g}^{-1} = \begin{pmatrix} g_1 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ g_n \end{pmatrix} \circ \begin{pmatrix} e_{G_1} \\ \vdots \\ e_{G_{j-1}} \\ g'_j \\ e_{G_{j+1}} \\ \vdots \\ e_{G_n} \end{pmatrix} \circ \begin{pmatrix} g_1^{-1} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ g_n^{-1} \end{pmatrix} = \begin{pmatrix} e_{G_1} \\ \vdots \\ e_{G_{j-1}} \\ g_j g'_j g_j^{-1} \\ e_{G_{j+1}} \\ \vdots \\ e_{G_n} \end{pmatrix} \in \varphi_j(G_j)$
- $\psi_j : \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} \overset{G \to G_j}{\mapsto} g_j$ ist surjektiver Homomorphismus von Gruppen.
  - Beweis: klar
- universelle Eigenschaft des direkten Produkts: Seien $\eta_i : H \to G_i$ Homomorphismen von Gruppen, dann: Es gibt genau einen Homomophismus von Gruppen $\Phi : H \to G$ mit $\eta_j = \psi_j \circ \Phi \forall 1 \le j \le n$, also so, dass dieses Diagramm kommutiert:



  - Beweis: Definiere $\Phi(h) := \begin{pmatrix} \eta_1(h) \\ \vdots \\ \eta_n(h) \end{pmatrix}$.
- N_1, N_2 Untergruppen von einer Gruppe G, dann:

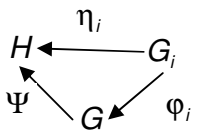
$N_1 \times N_2 \to G$

$\iota : \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \mapsto n_1 n_2$ ist Isomorphismus von Gruppen

$\Leftrightarrow \forall g \in G \exists g_1,\ldots,g_r \in N_1 \cup N_2 : g = g_1 \cdot \ldots \cdot g_r \wedge N_1, N_2 \lhd G \wedge N_1 \cap N_2 = \{e\}$

- Definition 'inneres, direktes Produkt von N_1 und N_2': die obigen Bedingungen gelten, Schreibweise $G = N_1 \times N_2$
- Definition 'direkte Summe $\coprod_{i=1}^{n} G_i$': $\coprod_{i=1}^{n} G_i := G_1 \oplus \ldots \oplus G_n = \left\{ \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} \middle| g_i = e_{G_i} \text{ für fast alle } g_i \right\}$

  ($n = \infty$ zulässig)
- Falls $n < \infty$, so ist $\coprod_{i=1}^{n} G_i = \prod_{i=1}^{n} G_i$.
- $G := \coprod_{i=1}^{n} G_i$, $\circ : \left(\begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix}, \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} \right) \mapsto \begin{pmatrix} g_1 h_1 \\ \vdots \\ g_n h_n \end{pmatrix}$, dann: $(G, \circ)$ ist Gruppe.
- $\varphi_j : \begin{matrix} G_j \to G \\ g_j \mapsto \end{matrix} \begin{pmatrix} e_{G_1} \\ \vdots \\ e_{G_{j-1}} \\ g_j \\ e_{G_{j+1}} \\ \vdots \\ e_{G_n} \end{pmatrix}$ ist injektiver Homomorphismus von Gruppen.
- $\varphi_j(G_j) \cong G_j \wedge \varphi_j(G_j) \lhd G$:
- $\psi_j : \begin{matrix} G \to G_j \\ \end{matrix} \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} \mapsto g_j$ ist surjektiver Homomorphismus von Gruppen.
- universelle Eigenschaft der direkten Summe: Seien $\eta_i : G_i \to H$ Homomorphismen von Gruppen, dann: Es gibt genau einen Homomophismus von Gruppen $\Psi : G \to H$ mit $\eta_j = \Psi \circ \varphi_j \forall 1 \le j \le n$, also so, dass dieses Diagramm kommutiert:



  - Beweis: Definiere $\Psi\left(\begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} \right) := \prod_{j=1}^{n} n_j(g_j)$.
- Definition 'Automorphismengruppe von G $\mathrm{Aut}(G)$':

$\mathrm{Aut}(G) := \{f : G \to G \mid f \text{ ist Isomorphismus von Gruppen}\}$

- $\mathrm{Aut}(G)$ ist Gruppe bzgl. der Komposition (Hintereinanderausführung) von Funktionen $\circ$.
  - Beweis: klar
- Definition 'semidirektes Produkt von G und H bzgl. φ $(G \times_\varphi H, \circ)$' ($\varphi : H \to \mathrm{Aut}(G)$ Homomorphismus von Gruppen): $\circ : \begin{matrix}(G \times H) \times (G \times H) \to G \times H \\ \left(\begin{pmatrix} g_1 \\ h_1 \end{pmatrix}, \begin{pmatrix} g_2 \\ h_2 \end{pmatrix}\right) \mapsto \begin{pmatrix} g_1 \cdot \varphi(h_1)(g_2) \\ h_1 h_2 \end{pmatrix}\end{matrix}$
- $(G \times_\varphi H, \circ)$ ist eine Gruppe.
  - Beweis:
    - Assoziativität: nachrechnen
    - neutrales Element: $\begin{pmatrix} e_G \\ e_H \end{pmatrix}$
    - inverses Element: $\begin{pmatrix} g \\ h \end{pmatrix}^{-1} = \begin{pmatrix} \varphi(h^{-1})(g^{-1}) \\ h^{-1} \end{pmatrix}$
- $(\{e_G\} \times H)$ und $\{G \times \{e_H\}\}$ sind Untergruppen von $G \times_\varphi H$
  - Beweis: nachrechnen
- $(G \times_\varphi H, \circ)$ kommutativ $\Leftrightarrow G, H$ kommutativ $\wedge\, \varphi = \mathrm{id}_G$
  - Beweis: nachrechnen
- $(G \times_\varphi H, \circ) = (G \times H, \circ) \Leftrightarrow \varphi = \mathrm{id}_G$
  - Beweis: nachrechnen

4.2 Presentationen

- Definition 'von $M = \{g_1, \ldots\} \subseteq G$ erzeugte Untergruppe von G $\langle M \rangle$': $\langle M \rangle := \left(\left\{a_1 \circ \ldots \circ a_r \mid a_i \in M \vee a_i^{-1} \in M\right\}, \circ\right)$
- $G_1, \ldots$ Untergruppen $\Rightarrow \bigcap G_i$ Untergruppe
  - Beweis: $g_1, g_2, g \in \bigcap G_i \Rightarrow g_1, g_2, g \in G_i \forall i \Rightarrow g_1 \circ g_2, g^{-1} \in G_i \forall i \Rightarrow g_1 \circ g_2, g^{-1} \in \bigcap G_i$
- Sei $\{G_1, \ldots\}$ die Menge aller Untergruppen, die $M \subseteq G$ enthalten, dann: $\langle M \rangle = \bigcap G_i$
  - Beweis:
    - '$\subseteq$': $a_1 \circ \ldots \circ a_r \in \langle M \rangle \Rightarrow a_i \in M \vee a_i^{-1} \in M \Rightarrow a_i \in \bigcap G_i \vee a_i^{-1} \in \bigcap G_i \Rightarrow a_i \in \bigcap G_i$
    - '$\supseteq$': $M \subseteq G_i \forall i \Rightarrow \langle M \rangle \subseteq G_i \forall i \Rightarrow \langle M \rangle \subseteq \bigcap G_i$
- Definition 'Alphabet Σ: Σ Menge; '$M(\Sigma)$' (Σ Menge): $M(\Sigma) := \{(x_1, \ldots, x_n) \mid n \geq 0, x_i \in \Sigma\}$; '$\circ : M(\Sigma) \times M(\Sigma) \to M(\Sigma)$': $\circ : \begin{matrix} M(\Sigma) \times M(\Sigma) \to M(\Sigma) \\ ((x_1, \ldots, x_n), (y_1, \ldots, y_m)) \mapsto (x_1, \ldots, x_n, y_1, \ldots, y_m) \end{matrix}$; 'reduziertes Element $(x_1, \ldots, x_n) \in M(\Sigma \cup \tilde{\Sigma})$' ($\tilde{\Sigma}$ weitere Menge, $\iota : \Sigma \to \tilde{\Sigma}$ bijektiv): Es gibt kein $i \in \{1, \ldots, n-1\} : x_{i+1} = \iota(x_i) \vee x_i = \iota(x_{i+1})$.; 'elementarer Reduktionsschritt eines nicht reduzierten Elements $(x_1, \ldots, x_n) \in M(\Sigma \cup \tilde{\Sigma})$': $(x_1, \ldots, x_n) \to (x_1, \ldots, x_{i-1}, x_{i+2}, \ldots, x_n) \in M(\Sigma \cup \tilde{\Sigma})$; 'Äquivalenzrelation ~ auf $M[\Sigma \cup \tilde{\Sigma}]$': die durch elementare Reduktionsschritte erzeugte Äquivalenzrelation, d. h. $w_1 := (x_1, \ldots, x_n)$, $w_r := (y_1, \ldots, y_m)$ und $w_i \to w_{i+1} \vee w_{i+1} \to w_i$; 'freies Monoid bzgl. dem Alphabet Σ':

$(M(\Sigma),\circ)$

- $(M(\Sigma),\circ)$ ist Monoid mit neutralem Element $e := (\ )$
- Definition 'freie Gruppe über dem Alphabet Σ $F(\Sigma)$': $F(\Sigma) := \left(\underbrace{M(\Sigma \cup \tilde{\Sigma})/\sim}_{\text{Menge der Äquivalenzklassen}}, \circ \right)$ mit
  $\circ : \begin{matrix} (M(\Sigma \cup \tilde{\Sigma})/\sim) \times (M(\Sigma \cup \tilde{\Sigma})/\sim) \to M(\Sigma \cup \tilde{\Sigma})/\sim \\ ([(x_1,\ldots,x_n)],[(y_1,\ldots,y_m)]) \mapsto [(x_1,\ldots,x_n,y_1,\ldots,y_m)] \end{matrix}$; '$x^{-1} \in \tilde{\Sigma}$': $x^{-1} := \iota(x)$; 'Σ^{-1}': $\Sigma^{-1} := \tilde{\Sigma}$;
  'Wort über dem Alphabet Σ': ein Element aus $M(\Sigma \cup \Sigma^{-1})$; '$\Sigma^*$': $\Sigma^* := M(\Sigma \cup \Sigma^{-1})$;
  '$x_1 \cdots x_n$': $x_1 \cdots x_n := [(x_1,\cdots,x_n)] \in F(\Sigma)$
- $F(\Sigma)$ ist Gruppe.
  - Beweis:
    - Assoziativität: Da die Konkatenation an sich assoziativ ist.
    - neutrales Element: $[e] = [(\ )]$
    - inverses Element: $[(x_1,\ldots,x_n)]^{-1} = \left[\left(x_n^{-1},\ldots,x_1^{-1}\right)\right]$
- $\Sigma := \{x\} \Rightarrow F(\Sigma) \cong Z$
  - Beweis: Benutze den Isomorphismus $\left[\left(\underbrace{x,\ldots,x}_{i \text{ Stück}}\right)\right] \mapsto i, \left[\left(\underbrace{x^{-1},\ldots,x^{-1}}_{i \text{ Stück}}\right)\right] \mapsto -i$
- universelle Eigenschaft der freien Gruppe: H Gruppe, $f : \Sigma \to H$, dann: Es gibt einen eindeutigen Homomorphismus von Gruppen $\varphi : \begin{matrix} F(\Sigma) \to H \\ x \mapsto f(x) \end{matrix}$.
  - Beweis: Setze $\varphi(x_i) := \begin{cases} f(x_i), \text{falls } x_i \in \Sigma \\ \left(f\left(x_i^{-1}\right)\right)^{-1}, \text{falls } x_i \in \Sigma^{-1} \end{cases}$ und $\varphi(x_1 \cdots x_n) := \varphi(x_1) \cdots \varphi(x_n)$.
- Es gibt einen eindeutig bestimmten, surjektiven Homomorphismus von Gruppen $\varphi : \begin{matrix} F(M) \to \langle M \rangle \\ x \mapsto x \end{matrix}$. Insbesondere ist $\langle M \rangle \cong F(M)/\ker\varphi$.
- Definition 'Presentation von $G := \langle M \rangle$': der Isomorphismus $\langle M \rangle \cong F(M)/\ker\varphi$

5. Kommutative Gruppen

5.1 Zyklische Gruppen

- $n := \mathrm{ord}_G(g) < \infty$, dann:
  - $g^m = e \Rightarrow n \mid m$
    - Beweis:
      - Eigentlich klar, denn g wird immer erst nach n Multiplikationen wieder e, d. h. m muss offensichtlich ein Vielfaches von n sein.
      - $m \underbrace{=}_{\text{Division mit Rest}} pn + r$
      - $e = g^m = g^{np+r} = \underbrace{\left(g^n\right)^p}_{=e} \cdot g^r = g^r \underbrace{\Rightarrow}_{r \underbrace{\leq}_{r \text{ ist Rest der Division}} n = \mathrm{ord}_G(g)} r = 0$
  - $m \mid n \Rightarrow \mathrm{ord}_G\left(g^m\right) = \frac{n}{m}$

  - Beweis: $\left(g^m\right)^{\frac{n}{m}} = g^n = e$
- $\langle g \rangle = \{e, g, \ldots, g^{n-1}\}$ und $\#\langle g \rangle = n$
  - Beweis: klar
- G endlich $\Rightarrow$ $n \mid \#G$
  - Beweis: $\#\langle g \rangle = n$ und $\#\langle g \rangle \mid \#G$ nach Satz von Lagrange, also $n \mid \#G$
- $\mathrm{ord}_G\left(g^k\right) = \dfrac{n}{\mathrm{ggT}(n,k)} = \dfrac{\mathrm{kgV}(n,k)}{k}$
  - Beweis:
    - einerseits: $\left(g^k\right)^{\frac{n}{\mathrm{ggT}(n,k)}} = \underbrace{\left(g^n\right)}_{=e}^{\frac{k}{\mathrm{ggT}(n,k)}} = e$
    - andererseits: $\left(g^k\right)^{\frac{n}{\mathrm{ggT}(n,k)}} = g^{\frac{nk}{\mathrm{ggT}(n,k)}} = g^{\mathrm{kgV}(n,k)}$, d. h. erst $\left(g^k\right)^{\frac{n}{\mathrm{ggT}(n,k)}} = e$
- $n := \mathrm{ord}_G(g) < \infty$, $m := \mathrm{ord}_G(h) < \infty$, $gh = hg$ und $\mathrm{ggT}(n,m) = 1$, dann $\mathrm{ord}_G(gh) = nm$.
  - Beweis:
    - $(gh)^{nm} = \left(g^n\right)^m \cdot \left(h^m\right)^n = e$
    - Wegen $\mathrm{ggT}(n,m) = 1$ ist $\mathrm{kgV}(n,m) = nm$, also $\mathrm{ord}_G(gh) = nm$.
- Definition 'Exponent von G $\mathrm{Expo}(G)$': $\mathrm{Expo}(G) := \mathrm{kgV}\left(\mathrm{ord}_G(g) \mid g \in G\right)$
- $g^{\mathrm{Expo}(G)} = e$
  - Beweis: klar
- G kommutativ $\Rightarrow$ $\exists g \in G : \mathrm{ord}_G(g) = \mathrm{Expo}(G)$:
  - Beweis:
    - Zerlege $\mathrm{Expo}(G)$ in seine Primfaktorzerlegung, also $\mathrm{Expo}(G) = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$.
    - $\forall 1 \le i \le r \exists g \in G : \mathrm{ord}_G(g) = p_i^{\alpha_i} \cdot q_i$, d. h. $\mathrm{ord}_G(g)$ ist Vielfaches von $p_i^{\alpha_i}$, denn angenommen $\exists 1 \le i \le r \forall g \in G : \mathrm{ord}_G(g) = p_i^{\alpha_i'} \cdot q_i$ mit $0 \le a_i' < \alpha_i$, dann wäre $\mathrm{Expo}(G) = \mathrm{kgV}\left(\mathrm{ord}_G(g) \mid g \in G\right) = p_1^{\alpha_1} \cdot \ldots \cdot p_i^{\alpha_i'} \cdot \ldots \cdot p_r^{\alpha_r}$.
    - Hierbei gilt natürlich, dass in q_i der Primfaktor p_i nicht vorkommt. Also $\mathrm{ggT}\left(p_i^{\alpha_i}, q_i\right) = 1$
    - Wähle also entsprechende g_i-s mit $\mathrm{ord}_G(g_i) = p_i^{\alpha_i} \cdot q^i$
    - Somit $\mathrm{ord}_G\left(g_i^{q_i}\right) = p_i^{\alpha_i}$.
    - Wegen $\mathrm{ggT}\left(p_1^{\alpha_i}, \ldots, p_r^{\alpha_r}\right) = 1$, gilt $\mathrm{ord}_G\left(g_1^{q_1} \cdot \ldots \cdot g_r^{q_r}\right) = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} = \mathrm{Expo}(G)$.
- R Integritätsring, und G endliche Untergruppe von $(R \setminus \{0\}, \cdot)$ dann: G ist zyklisch.
- G endliche, zyklische Gruppe, $n := \#G$, dann: Zu jedem Teiler d von n gibt es genau eine Untergruppe U von G mit $\#U = d$
  - Beweis: Seien $G = \langle g \rangle$ und $m = \dfrac{n}{d}$, dann: $\mathrm{ord}_G\left(g^m\right) = d$, also $U := \left\{e, \left(g^m\right), \ldots, \left(g^m\right)^{d-1}\right\} = \left\{e, g^m, \ldots, g^{(d-1)m}\right\}$ und $\#U = d$.

5.2 Endlich erzeugte, kommutative Gruppen (additive Notation)

- Definition 'Basis von G $\{g_1, \ldots, g_r\}$': Für alle g-s gibt es eine Darstellung $g = a_1 g_1 + \ldots + a_r g_r$.; 'freie, kommutative/ Abelsche Gruppe': Es gibt eine Basis.;

Definition ‘Rang von G $\mathrm{rk}(G)$’: $\mathrm{rk}(G)=r$

- $\varphi: \begin{array}{ccc} G & \to & Z^r \\ a_1g_1+\ldots+a_rg_r & \mapsto & \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix} \end{array}$ ist ein Isomorphismus von Gruppen.
  - Beweis: klar
- $\{h_1,\ldots,h_s\}$ weitere Basis von G, dann: $s=r$.
- Hauptsatz für freie, kommutative Gruppen: $\mathrm{rk}(G)=r$, U Untergruppe, dann: Es gibt eine Basis $\{g_1,\ldots,g_r\}$ von G, $s\le r$ und Zahlen $\varepsilon_1,\ldots,\varepsilon_s\in\mathbb{N}$, so dass $\varepsilon_1\mid\varepsilon_2,\ldots,\varepsilon_{s-1}\mid\varepsilon_s$ und $\{\varepsilon_1g_1,\ldots,\varepsilon_sg_s\}$ eine Basis von U ist.
- Hauptsatz für endlich erzeugte, kommutative Gruppen:
  - Es gibt $r\ge 0,\varepsilon_1,\ldots,\varepsilon_s\in\mathbb{N}:\varepsilon_1>1\wedge\varepsilon_1\mid\varepsilon_2,\ldots,\varepsilon_{s-1}\mid\varepsilon_s$ und $G\cong Z^r\oplus Z/\varepsilon_1Z\oplus\ldots\oplus Z/\varepsilon_sZ$.
  - r ist eine Invariante von G und ist der Rang von G.
  - G endlich $\Rightarrow$ $r=0\wedge\varepsilon_s=\mathrm{Expo}(G)$. (Hier ist auch ε_s eine Invariante von G.)
- Definition ‘Elementarteiler von G’: die $\varepsilon_1,\ldots,\varepsilon_s$ von eben; ‘Torsionsuntergruppe von G $T(G)$’: $T(G):=\{g\in G\mid \mathrm{ord}_G(g)<\infty\}$
- G endlich erzeugte, kommutative Gruppe und $\psi: G\tilde{\to} Z^r\oplus Z/\varepsilon_1Z\oplus\ldots\oplus Z/\varepsilon_sZ$ der nach dem ‘Hauptsatz für endlich erzeugte, kommutative Gruppen’ existierende Isomorphismus, dann:
  - $T(G)=\psi^{-1}\left(\underbrace{\begin{pmatrix}0\\\vdots\\0\end{pmatrix}}_{\in Z^r}\oplus Z/\varepsilon_1Z\oplus\ldots\oplus Z/\varepsilon_sZ\right)$
  - $\varepsilon_1,\ldots,\varepsilon_s$ sind Invarianten von G.
- Definition ‘torsionsfrei’: $T(G)=0$
- G torsionsfrei $\Rightarrow$ G frei
  - Beweis:

$$T(G)=0_G\Leftrightarrow\psi^{-1}\left(\underbrace{\begin{pmatrix}0\\\vdots\\0\end{pmatrix}}_{\in Z^r}\oplus Z/\varepsilon_1Z\oplus\ldots\oplus Z/\varepsilon_sZ\right)=0_G$$

$$\underbrace{\Leftrightarrow}_{\text{weil }\psi\text{ Isomorphismus ist, ist }\ker(\psi)=0}\underbrace{\begin{pmatrix}0\\\vdots\\0\end{pmatrix}}_{\in Z^r}\oplus Z/\varepsilon_1Z\oplus\ldots\oplus Z/\varepsilon_sZ=0_{Z^r\oplus Z/\varepsilon_1Z\oplus\ldots\oplus Z/\varepsilon_sZ}$$

$$\Leftrightarrow Z/\varepsilon_1Z\oplus\ldots\oplus Z/\varepsilon_sZ=0_{Z^r\oplus Z/\varepsilon_1Z\oplus\ldots\oplus Z/\varepsilon_sZ}$$

$$\underbrace{\Rightarrow}_{G\cong Z^r\oplus Z/\varepsilon_1Z\oplus\ldots\oplus Z/\varepsilon_sZ}\quad G\cong Z^r\Leftrightarrow G\text{ ist frei.}$$

- der chinesische Restsatz: Seien $n_1,\ldots,n_s\in\mathbb{N}:\mathrm{ggT}(n_i,n_j)=1$ und $N:=n_1\cdot\ldots\cdot n_s$, dann:

$Z/nZ \tilde{\to} Z/n_1Z \times \ldots \times Z/n_sZ$

- $\varphi: \quad a+NZ \mapsto \begin{pmatrix} a+n_1Z \\ \vdots \\ a+n_sZ \end{pmatrix}$ ist ein Isomorpismus.
- φ induziert einen Isomorphismus multiplikativer Gruppen $\psi: (Z/NZ)^\times \tilde{\to} (Z/n_1Z)^\times \times \ldots \times (Z/n_sZ)^\times$

- G endlich und kommutativ, $n := \#G$, $m \mid n$, dann: Es gibt Untergruppe U mit $\#U = m$.
- Klassifikation endlicher, kommutativer Gruppen: $n = p_1^{\alpha_1} \cdot \ldots \cdot p_e^{\alpha_r}$ (Primfaktorzerlegung), $A\left(p_i^{\alpha_i}\right) := \#\text{Partitionen } \alpha_i = \alpha_{i1} + \ldots + \alpha_{ik} \mid 1 \le \alpha_{i1} \le \ldots \le \alpha_{ik}$, dann: Es gibt (bis auf Isomorphie) genau $A(n) = A\left(p_1^{\alpha_1}\right) \cdot \ldots \cdot A\left(p_r^{\alpha_r}\right)$ verschiedene Gruppen der Ordnung n.

6. p-Gruppen

6.1 Der Satz von Cauchy

- Definition 'p-Gruppe' (p Primzahl): $\forall g \exists n: \operatorname{ord}_G(g) = p^n$
- $\#G = p^n \Rightarrow G$ ist p-Gruppe. ('$\Leftarrow$' gilt auch, siehe unten)
  - Beweis: Nach dem kleinen Fermat's Satz gilt $\operatorname{ord}_G(g) \mid p^n \Rightarrow \operatorname{ord}_G(g) = p^m$
- $\#G = p^n \Rightarrow Z(G) \neq \{e\}$
  - Beweis:
    - $\#G = \#Z(G) + \sum_{\{i \mid [G:Z(g_i)] > 1\}} [G:Z(g_i)]$ (Klassengleichung)
    - $\#Z(G) = \underbrace{\underbrace{\#G}_{\text{Vielfaches von } p} - \underbrace{\sum_{\{i \mid [G:Z(g_i)] > 1\}} \underbrace{[G:Z(g_i)]}_{\text{Vielfaches von } p \text{ nach Satz von Lagrange}}}_{\text{Vielfaches von } p}}_{\text{Vielfaches von } p} \Rightarrow p \mid \#Z(G) \Rightarrow \#Z(G) \ge p > 1$
- $\#G = p^n$, G operiere auf einer Menge M, M^G die Menge der Fixpunkte dieser Operation, dann: $\#M^G \equiv \#M \bmod p$
  - Beweisidee:
    - $M = \left(\dot{\bigcup_{i=1}^{r}} Gm_i\right) \dot{\cup} M^G$ (disjunkte Vereinigung der Bahnen)
    - $\#(Gm_i) \mid \#G$ (wegen $\#G = \#(Gm) \cdot \#(G_{\{m\}})$, s. Kapitel 3) $\underset{\#Gm_i > 1, \text{ weil sonst } m_i \text{ Fixpunkt wäre}}{\Rightarrow}$ $p \mid \#(Gm_i)$
    - also $\#M = \underbrace{\#\left(\sum_{i=1}^{r} \underbrace{\#Gm_i}_{\equiv 0 \bmod p}\right)}_{\equiv 0 \bmod p} + \#M^G \Rightarrow \#M \equiv \#M^G \bmod p$
- Satz von Cauchy: $q \mid \#G \Rightarrow \exists g: \operatorname{ord}_G(g) = q$
- $\#G = p^n \Leftrightarrow G$ ist p-Gruppe.
  - '$\Rightarrow$': Bereits gezeigt.
  - '$\Leftarrow$':

- Angenommen, es gibt eine weitere Primzahl q, die $\#G$ teilt.
- Dann folgt mit dem Satz von Cauchy: $\mathrm{ord}_G(g) = q$. Widerspruch zur Definition der p-Gruppe.

6.2 Die Sätze von Sylow

- Frage: $m \mid G \overset{?}{\Rightarrow} \exists U : \#U = m$:
  - ja, für kommutative Gruppen (sogar eindeutig, wenn G zyklisch ist)
  - nein im Allgemeinen
- Definition 'p-Sylowuntergruppe von G' (p Primzahl): eine bzgl. Inklusion maximale p-Untergruppe von G
- Lemma von Zorn: M partiell geordnete Menge, $\forall (m_1 \le m_2 \le \ldots) \exists m : m_i \le m \forall i$, dann: M besitzt ein maximales Element.
- Definition 'p-Torsion': $T_p(G) := \left\{ g \in G \middle| \exists n : \mathrm{ord}_G(g) = p^n \right\}$
- Existenz von p-Sylowuntergruppen:
  - Es gibt eine p-Sylowuntergruppe.
    - Beweis:
      - Sei M die Menge aller p-Untergruppen. $\{e\} \in M$ ist p-Untergruppe.
      - Sei $U_1 \subseteq U_2 \subseteq \ldots$ eine beliebige Kette von p-Untergruppen, dann ist auch $U := \bigcup_i U_i$ p-Untergruppe.
      - Es gilt $U_i \subseteq U \forall i$, also ist U eine obere Schranke.
      - Nach Zorn's Lemma besitzt M ein maximales Element.
  - G kommutativ $\Rightarrow$ Es gibt genau 1 p-Sylowuntergruppe, nämlich $T_p(G)$.
    - Beweis: $T_p(G)$ ist p-Untergruppe, denn $\left(\underbrace{g}_{\in T_p(G)} \underbrace{h}_{\in T_p(G)} \right)^{p^{\overbrace{n}^{\mathrm{ord}_G(g)} + \overbrace{m}^{\mathrm{ord}_G(h)}}} = g^{p^{n+m}} \cdot h^{p^{n+m}} = e \Rightarrow \exists k \, \mathrm{ord}_G((gh)) = p^k \Rightarrow (gh) \in T_p(G)$, und maximal nach Defintion.
- U p-Sylowuntergruppe $\Rightarrow$ gUg^{-1} p-Sylowuntergruppe
  - Beweis:
    - Angenommen, es gäbe eine p-Untergruppe V mit $gUg^{-1} \subset V$.
    - dann: $U \subset g^{-1}Vg$
    - Das darf aber nur sein, wenn $g^{-1}Vg$ keine p-Gruppe ist, denn U ist ja eine maximale p-Gruppe nach Voraussetzung.
    - $g^{-1}Vg$ ist aber p-Gruppe, denn:
      - Sei v beliebig und $\mathrm{ord}_G(v) = p^n$ (geht, da V nach Annahme p-Untergruppe ist).
      - dann: $(g^{-1}vg)^{p^n} = (g^{-1}vg)(g^{-1}vg)\ldots(g^{-1}vg) = g^{-1}v^{p^n}g = g^{-1}eg = e$
      - daher: $\exists k \, \mathrm{ord}_G((g^1vg)) = p^k$
      - also: $g^{-1}Vg$ ist p-Gruppe.
- Hat G nur eine p-Sylowuntergruppe, so ist diese ein Normalteiler.
  - Es gilt 'U p-Sylowuntergruppe $\Rightarrow$ gUg^{-1} p-Sylowuntergruppe'.
  - Da es nur eine gibt, ist $U = gUg^{-1}$, also Normalteiler.

- U p-Untergruppe und $N(U) = \{g \in G \mid gUg^{-1} = U\}$ ihr Normalisator, dann:
  - $[N(U):U] \equiv [G:U] \bmod p$
  - $p \mid [G:U] \Rightarrow N(U) \neq U$
- 1. Satz von Sylow: $\#G = p^n \cdot m$ (in m ist p nicht mehr als Primfaktor vorhanden), dann:
  - $\forall 0 \le i \le n \exists U : \mathrm{ord}(U) = p^i$. Insbesondere: U p-Sylowuntergruppe $\Rightarrow \mathrm{ord}(U) = p^n$.
  - $0 \le i \le n-1 \wedge \mathrm{ord}(U_1) = p^i \Rightarrow \exists U_2 : \mathrm{ord}(U_2) = p^{i+1} \wedge U_1 \lhd U_2$
- 2. Satz von Sylow: U, V p-Sylowuntergruppen, dann: $\exists g : V = gUg^{-1}$, d. h. je 2 p-Sylowuntergruppen sind zueinander konjugiert.
- 3. Satz von Sylow: $\#G = p^n \cdot m$ (in m ist p nicht mehr als Primfaktor vorhanden), s_p die Anzahl der p-Sylowuntergruppen, dann:
  - $s_p \mid m$
  - $s_p \equiv 1 \bmod p$

7. Auflösbare Gruppen

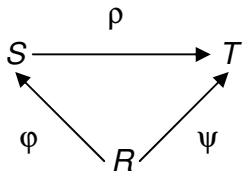
- Definition 'G ist auflösbar': Es gibt $\{e\} =: N_0 \subseteq N_1 \subseteq \ldots \subseteq N_l := G$, so dass für alle i gilt:
  - N_i ist Untergruppe
  - $N_{i-1} \lhd N_i$
  - N_i / N_{i-1} ist kommutativ.
- G kommutativ $\Rightarrow$ G auflösbar
  - Beweisidee: die Kette $\{e\} =: N_0 \subseteq N_1 := G$
- Definition 'einfache Gruppe': Die einzigen Normalteiler sind $\{e\}$ und G.
- G nicht kommutativ und einfach $\Rightarrow$ G nicht auflösbar
  - Beweis:
    - Einzig mögliche Kette ist $\{e\} =: N_0 \subseteq N_1 := G$, weil nur $\{e\}$ und G Normalteiler sind.
    - Aber $N_1 / N_0 = G/\{e\} \cong G$ ist nicht kommutativ.
- G endliche p-Gruppe $\Rightarrow$ G auflösbar
  - Beweis: Folgt aus dem 1. Satz von Sylow
- Definition 'Normalreihe von G': eine Kette von Untergruppen $\{e\} =: N_0 \subseteq N_1 \subseteq \ldots \subseteq N_l := G$ mit $N_{i-1} \lhd N_i$
- G auflösbar, dann:
  - U Untergruppe, dann U auflösbar
    - Beweisidee: die Kette $\{e\} = N_0 \cap U \subseteq N_1 \cap U \subseteq \ldots \subseteq N_l \cap U = U$
  - $U \lhd G \Rightarrow G/U$ auflösbar
    - Beweisidee: die Kette $\{e\} = N_0U/U \subseteq N_1U/U \subseteq \ldots \subseteq N_lU/U = G/U$
- G endlich erzeugt, dann: Es gibt eine Normalreihe $\{e\} =: N_0 \subseteq N_1 \subseteq \ldots \subseteq N_l := G$ mit zyklischen Restklassengruppen N_i / N_{i-1}.
- G endlich und kommutativ, dann: Es gibt eine Normalreihe $\{e\} =: N_0 \subseteq N_1 \subseteq \ldots \subseteq N_l := G$ mit zyklischen Restklassengruppen N_i / N_{i-1} von Primzahlordnung.
- G endlich und auflösbar und $N \lhd G$, dann: Es gibt eine Normalreihe $\{e\} =: N_0 \subseteq N_1 \subseteq \ldots \subseteq N_l := G$ mit folgenden Eigenschaften:

- N_i / N_{i-1} ist zyklisch von Primzahlordnung
- $N \in \{N_0, \ldots, N_l\}$

- G einfach und auflösbar, dann: G ist zyklisch von Primzahlordnung:
  - Beweis: Folgt aus eben Gezeigtem.
- A_n wird für $n \geq 3$ von den Dreierzyklen $\sigma_{abk} = \begin{pmatrix} 1 & \cdots & a & \cdots & b & \cdots & k & \cdots & n \\ 1 & \cdots & b & \cdots & k & \cdots & a & \cdots & n \end{pmatrix}$ erzeugt.
- $n \geq 3$, $N \lhd A_n$, N enthält einen Dreierzyklus, dann: $N = A_n$.
  - Beweis:
    - Seien $\sigma_{abc} \in N$ und σ_{abk} ein beliebiger Dreierzyklus.
    - Es gilt: $\sigma_{abk} = (\tau_{ab}\tau_{ck})\sigma_{abc}^2(\tau_{ab}\tau_{ck})^{-1}$.
    - außerdem: $\sigma_{abk} = (\tau_{ab}\tau_{ck})\sigma_{abc}^2(\tau_{ab}\tau_{ck})^{-1} \in N$, weil $N \lhd A_n$
    - Also ist jeder beliebige Dreierzyklus in N.
    - Wegen ‘ A_n wird für $n \geq 3$ von den Dreierzyklen erzeugt.’ folgt $N = A_n$.
- $n \neq 4 \Rightarrow A_n$ ist einfache Gruppe.
- $n \geq 5 \Leftrightarrow S_n$ ist nicht auflösbar.

1.1 Polynomial Rings

- Definition ‘Halbgruppe’; ‘Monoid’; ‘Gruppe’; ‘Ring’; ‘Körper’
- Definition ‘nilpotent’: $r^i = 0$; ‘Nicht-Nullteiler’: $rr' = 0 \Rightarrow r' = 0 \Leftrightarrow$: r ist Nicht - Nullteiler
- Definition ‘Integritätsbereich’ (‘integral domain’): Alle Elemente ungleich 0 sind Nicht-Nullteiler.
- Definition ‘Ringhomomorphismus’:
  - $\varphi(1_R) = 1_S$
  - $\varphi(r + r') = \varphi(r) + \varphi(r')$
  - $\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')$
- Definition ‘R-Algebra’: ein weiterer Ring S zusammen mit einem Ringhomomorphismus (genannt Strukturhomomorphismus), der S mit R verbindet; ‘R-Algebren-Homomorphismus von 2 R-Algebren S und T ρ’: $\rho(\varphi(r) \cdot s) = \rho(\varphi(r)) \cdot \rho(s) = \psi(r) \cdot \rho(s)$



- Definition ‘R-Modul’: $\hat{=}$ Vektorraum für Ringe; ‘R-Untermodul’; ‘R-lineare Abbildung (zwischen 2 Moduln)’: $\varphi(m + m') = \varphi(m) + \varphi(m')$ und $\varphi(r \cdot m) = r \cdot \varphi(m)$; ‘Ideal’: einmal Standard-Definition ($R \cdot I \subseteq I$), einmal als R-Untermodul des R-Moduls R
- Ist R sogar ein Körper, so gibt es nur die Ideale R und $\langle 0 \rangle$.:
  - Beweis: I Ideal; $i \in I$; da R Körper existiert i^{-1}; da I Ideal: $i^{-1} \cdot i = 1 \in I$; da I Ideal $r \in R \Rightarrow r \cdot \underbrace{1}_{\in I} = r \in I$, also $R \subseteq I$; da sowieso $I \subseteq R$, ist $I = R$
- R/I ist ein R-Modul (mit dem Skalarprodukt $\left(\underbrace{r}_{\in R}, \underbrace{\bar{s}}_{\in R/I} \right) \mapsto \overline{rs}$) und – zusammen mit der kanonischen Abbildung $R \to R/I$ – auch eine R-Algebra (R/I ist auch ein Ring).
- Definition ‘Primideal’: $s \in I$ und $s = \underbrace{r}_{R} \cdot \underbrace{r'}_{R}$, so folgt $r \in I \vee r' \in I$; ‘maximales Ideal’: Erweitert man I zu einem echt größeren Ideal, so erhält man R.
- I ist Primideal genau dann, wenn R/I ein Integritätsbereich ist.:
  - Beweis:
    - ‘$\Rightarrow$’: $\bar{r}_1 \cdot \bar{r}_2 = \bar{0} \Rightarrow r_1 \cdot r_2 \in I \underbrace{\Rightarrow}_{\text{da } I \text{ Primideal}} r_1 \in I \vee r_2 \in I \Rightarrow \bar{r}_1 = \bar{0} \vee \bar{r}_2 = \bar{0}$
    - ‘$\Leftarrow$’: $r_1 \cdot r_2 \in I \Rightarrow \bar{r}_1 \cdot \bar{r}_2 = \bar{0} \underbrace{\Rightarrow}_{\text{da } R/I \text{ Integritätsbereich}} \bar{r}_1 = \bar{0} \vee \bar{r}_2 = \bar{0} \Rightarrow r_1 \in I \vee r_2 \in I$
- I ist ein maximales Ideal genau dann, wenn R/I ein Körper ist.
- Jedes maximale Ideal ist ein Primideal.:
  - Beweis: I maximales Ideal $\Leftrightarrow$ R/I Körper $\Rightarrow$ R/I Integritätsbereich $\Leftrightarrow$ I Primideal
- Definition ‘Erzeugendensystem eines Moduls M $(m_1, \ldots)$’: $\forall m \in M \exists r_1, \ldots, r_n \in R, m_{i_1}, \ldots, m_{i_n} \in (m_1, \ldots) : m = r_1 m_{i_1} + \ldots + r_n m_{i_n}$; ‘endlich erzeugt’: $(m_1, \ldots)$ ist endliche Menge; ‘zyklisch erzeugter Modul’: Der Modul lässt sich durch ein einziges

Element erzeugen.; ‘Hauptideal’ (‘principal ideal’): Das Ideal lässt sich durch ein einziges Element erzeugen.; ‘R-Basis’: Jedes Element hat eine eindeutige Darstellung.; ‘freier Modul’: Es gibt eine R-Basis.; ‘Rang eines Moduls’: Anzahl der Erzeuger in einer **Basis**

- In $K[x]$ ist jedes Ideal ein Hauptideal.
- Notation für den Polynomring $\underbrace{R}_{\text{ein Ring}}[x]$: $r_0\underbrace{\begin{pmatrix}1\\0\\0\\0\\\vdots\end{pmatrix}}_{=e_0}+r_1\underbrace{\begin{pmatrix}0\\1\\0\\0\\\vdots\end{pmatrix}}_{=e_1}+r_2\underbrace{\begin{pmatrix}0\\0\\1\\0\\\vdots\end{pmatrix}}_{=e_2}+\ldots$ statt $r_0x^0+r_1x^1+r_2x^2+\ldots\ (r_i\in R)$
- Einbettung von R in $R[x]$ $\left(r\mapsto r\begin{pmatrix}1\\0\\0\\0\\\vdots\end{pmatrix}\right)$
- Definition ‘$R[x_1,\ldots,x_n]$’ (rekursiv): $R[x_1,\ldots,x_n]:=(R[x_1,\ldots,x_{n-1}])[x_n]$
- verschiedene Strukturen für $K[x_1,\ldots,x_n]$:
  - als Ring mit Erzeugendensystem $(x_1,\ldots,x_n)$ (Beispiel: $x_1^2+2x_1x_2=\underbrace{x_1x_1+x_1x_2+x_1x_2}_{\text{Ringoperationen}}$)
  - als K-Vektorraum mit Erzeugendensystem T^n (Definition von T^n siehe unten) (Beispiel: $x_1^2+2x_1x_2=\begin{pmatrix}0\\\vdots\\0\\\underbrace{2}_{\text{für Erzeuger } x_1x_2}\\0\\\vdots\\0\\\underbrace{1}_{\text{für Erzeuger } x_1^2}\\0\\\vdots\\0\end{pmatrix}$)
  - als (eindimensionaler) $K[x_1,\ldots,x_n]$-Modul mit Erzeugendensystem $\underline{1}$ (Beispiel: $x_1^2+2x_1x_2=\underbrace{\left(x_1^2+2x_1x_2\right)}_{\text{Element des Rings } K[x_1,\ldots,x_n]}\cdot\underline{1}$)
- Definition ‘Einheit’: $r\tilde{r}=1\Leftrightarrow$: r ist Einheit (Einheiten sind die invertierbaren Elemente.)
- R Integritätsbereich $\Rightarrow$ Die Einheiten in $R[x_1,\ldots,x_n]$ sind die Einheiten in R und $R[x_1,\ldots,x_n]$ ist ein Integritätsbereich.:

  - Wegen der rekursiven Definition von $R[x_1,\ldots,x_n]$ reicht ein Beweis für $n=1$.
  - $r = r_{d_r} x^{d_r} + \ldots \neq 0, s = s_{d_s} x^{d_s} + \ldots \neq 0 \in R[x] \Rightarrow rs = r_{d_r} s_{d_s} x^{d_r+d_s} + \ldots \underbrace{\neq}_{\substack{\text{weil } r_{d_r} s_{d_s} \neq 0, \\ \text{weil } R \text{ Integritätsbereich}}} 0$
  - Weil $d_r + d_s > 0$, ist $rs \notin R$ und somit definitiv nicht invertierbar, also keine Einheit.
- Representation eines multivarianten Polynoms:
  - streng nach der rekursiven Definition
  - mit Hilfe von Multi-Indizes
- Erzeugung von $M = (R[x_1,\ldots,x_n])^r$ als $R[x_1,\ldots,x_n]$-Modul und Basis $\left(\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix},\ldots,\begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix}\right)$
- Definition 'Term': Monom; 'T^n': Menge aller Terme mit *n* Variablen; 'Grad eines Terms': Summe der Potenzen; 'Logarithmus': Tupel der Potenzen; 'Term von $M = (R[x_1,\ldots,x_n])^r$': *r*-dimensionales Monom; '$T^n\langle e_1,\ldots,e_r\rangle$': Menge aller *r*-dimensionalen Terme mit *n* Variablen
- T^n ist ein kommutativer Monoid.
- Definition 'Koeffizient eines Terms'; 'Träger (Support) eines (mehrdimensionalen) Polynoms': Menge aller Terme, die im Polynom vorkommen; 'Grad eines eindimensionalen Polynoms': Grad des größten Terms des Polynoms
- Definition 'Auswertungshomomorphismus $\psi : R[x_1,\ldots,x_n] \to S$' ($\varphi : R \to S$, $s_1,\ldots,s_n \in S$): $\psi_{|R} = \varphi(r)$ und $\psi(x_i) = s_i$; 'Auswertung eines Polynoms *f* an einer Stelle $\vec{s}$ $f(\vec{s})$': $f(\vec{s}) := \psi(f)$; 'Ersetzungshomomorphismus' ('substitution homomorphism'): der Auswertungshomomorphismus, falls $S = R$ ist
- universelle Eigenschaft des Polynomrings: *S* *R*-Algebra, dann existiert ein eindeutiger Auswerungshomomorphismus für festes *s* bzw. feste s_i-s, nämlich $\psi(c_0 x^0 + \ldots + c_d x^d) := \varphi(c_0)s^0 + \ldots + \varphi(c_d)s^d$.
- Definition 'Erzeugendensystem einer *R*-Algebra $S := (s_1,\ldots)$': $\forall s \in S \exists \underbrace{s_1,\ldots,s_t}_{\text{endlich viele}}, f \in R[x_1,\ldots,x_t] : s = f(s_1,\ldots,s_t)$; 'endlich erzeugte *R*-Algebra'
- Endlich erzeugte *R*-Algebren *S* sind von der Form $S \cong R[x_1,\ldots,x_n]/\underbrace{I}_{\text{Ideal in } R[x_1,\ldots,x_n]}$, denn $\psi : R[x_1,\ldots,x_n] \to S$ ist surjektiv.
- Definition 'Presentation einer *R*-Algebra': der Isomorphismus $S \cong R[x_1,\ldots,x_n]/\underbrace{I}_{\text{Ideal in } R[x_1,\ldots,x_n]}$

1.2 Unique Factorization

- Definition 'reduzibel': $s = rr'$, weder *r* noch r' sind Einheiten; 'irreduzibel': nicht reduzibel; 'Faktorisierung': $r = \underbrace{u}_{\text{Einheit}} \cdot \underbrace{r_1 \cdot \ldots \cdot r_s}_{\text{irredzible Elemente}}$; 'Primelement': $r \mid r_1 r_2 \Rightarrow r \mid r_1 \vee r \mid r_2$
- In $K[x]$ ist ein Element, das keine Einheit ist (also ein 'echtes' Polynom und nicht nur eine Zahl aus dem Körper ist), Primelement genau dann, wenn es irreduzibel ist.
  - Beweis:

- '$\Rightarrow$':
  - $s = r_1 r_2 \Rightarrow s \mid r_1 r_2 \underbrace{\Rightarrow}_{\text{da prim}} s \mid r_1 \vee s \mid r_2 \Rightarrow \deg(s) \le \deg(r_1) \vee \deg(s) \le \deg(r_2)$
  - außerdem: $s = r_1 r_2 \Rightarrow \deg(s) \ge \deg(r_1) \wedge \deg(s) \ge \deg(r_2)$
  - insgesamt: $\deg(s) = \deg(r_1) \vee \deg(s) = \deg(r_2)$
  - wegen $s = r_1 r_2$: $\deg(s) = \deg(r_1) \wedge \deg(r_2) = 0 \vee \deg(s) = \deg(r_2) \wedge \deg(r_1) = 0$
  - also: r_2 Einheit oder r_1 Einheit
- '$\Leftarrow$':
  - $s \mid r_1 r_2 \Rightarrow \exists t : ts = r_1 r_2$
  - Annahme: $s \nmid r_1$. Dann zu zeigen $s \mid r_2$.
  - Betrachte das Ideal (r_1, s). Weil $K[x]$ Hauptidealring: $(r_1, s) = (1)$.
  - also:
    $\exists a, b : ar_1 + bs = 1 \Leftrightarrow ar_1 r_2 + bsr_2 = r_2 \Leftrightarrow ats + bsr_2 = r_2 \Leftrightarrow (at + br_2)s = r_2 \Leftrightarrow s \mid r_2$

- Defintion 'faktorieller Ring': Nicht-Einheiten haben eine eindeutige Faktorisierung.
- Jeder Körper ist trivialer Weise ein faktorieller Ring, denn es gibt keine Nicht-Einheiten.
- R ist faktoriell $\Leftrightarrow (r \in R$ ist irreduzibel $\Rightarrow r$ ist prim$)$
  - Beweis:
    - '$\Rightarrow$':
      - $r \mid r_1 r_2$. Da r irreduzibel ist, lässt sich r nicht aufspalten.
      - Also kann nicht ein Teil von r in r_1 stecken und der andere in r_2.
      - D. h. r kann r_1 oder r_2 nur als Ganzes teilen, d. h. $r \mid r_1 \vee r \mid r_2$.
    - '$\Leftarrow$':
      - $r = a_1 \ldots a_s = b_1 \ldots b_t \Rightarrow a_1 \mid b_1 \ldots b_t \underbrace{\Rightarrow}_{\text{nach Voraussetzung}}$ o. B. d. A. $a_1 \mid b_1$
      - Da a_1 und b_1 beide irreduzibel, folgt $a_1 = b_1$ (bis auf Einheiten).
      - also kürzen $a_2 \ldots a_s = b_2 \ldots b_t$ und induktiv fortfahren
      - Ergebnis: $s = t$ und $a_i = b_i$
- Definition 'ggT'; 'kgV'; 'relativ prim/ co-prim': $\text{ggT}(f_1, f_2) = 1$'; 'squarefree part von $f = c \cdot \underbrace{f_1^{\alpha_1} \cdot \ldots \cdot f_n^{\alpha_n}}_{\text{Faktorisierung von } f}$ $\text{sqfree}(f)$': $\text{sqfree}(f) := f_1 \cdot \ldots \cdot f_n$
- Charakterisierung 'ggT': $\text{ggT}(f_1, \ldots, f_m) = f \Leftrightarrow (f \mid f_i \wedge g \mid f_i \Rightarrow g \mid f)$; 'kgV': $\text{kgV}(f_1, \ldots, f_m) = f \Leftrightarrow (f_i \mid f \wedge f_i \mid g \Rightarrow f \mid g)$
- $\text{kgV}(f_1, \ldots, f_m)$ erzeugt das Ideal $(f_1) \cap \ldots \cap (f_m)$
- $\text{ggT}(f_1, f_2) \cdot \text{kgV}(f_1, f_2) = f_1 \cdot f_2$
- R Hauptidealring, dann: $\text{ggT}(f_1, \ldots, f_m)$ erzeugt $(f_1, \ldots, f_m)$; $\text{ggT}(f_1, \ldots, f_m) = 1 \Leftrightarrow \exists g_1, \ldots, g_m : g_1 f_1 + \ldots + g_m f_m = 1$
- Definition 'content eines Polynoms $\text{cont}(f)$': ggT der Koeffizienten; 'primitives Polynom': $\text{cont}(f) = 1$
- Gauß's Lemma: R faktorieller Ring, $f, g \in R[x] \setminus \{0\}$, dann: $\text{cont}(fg) = \text{cont}(f) \cdot \text{cont}(g)$ und $(f, g$ primitv $\Rightarrow fg$ primitiv$)$
- R faktorieller Ring, $f \in R[x] \setminus \{0\}$, dann: f besitzt eine Faktorisierung.
- R faktorieller Ring $\Rightarrow$ $R[x]$ faktorieller Ring

- K Körper $\Rightarrow$ $K[x_1,\ldots,x_n]$ faktorieller Ring

1.3 Monomial Ideals and Monomial Modules

- Definition 'Monoideal': $\hat{=}$ Ideal für Monoide; 'Erzeugendensystem eines Monoideals'; 'Monomodul'; 'Untermonomodul'; Erzeugendensystem eines Monomoduls'
- $T^n\langle e_1,\ldots,e_r\rangle$ ist ein T^n-Monomodul mit Erzeugendensystem $(e_1,\ldots,e_r)$.
- Definition 'Kürzungregel (cancellation law) für Monoide': $\gamma_1\circ\gamma_3=\gamma_2\circ\gamma_3\Rightarrow\gamma_1=\gamma_2$; 'Links-Kürzungsregel für Monomoduln': $\gamma\circ s_1=\gamma\circ s_2\Rightarrow s_1=s_2$; 'Rechts-Kürzungsregel für Monomoduln': $\gamma_1\circ s=\gamma_2\circ s\Rightarrow\gamma_1=\gamma_2$
- Γ Monoid, dann:
  Jedes Monoideal in Γ ist endlich erzeugt.
  $\Leftrightarrow$ Jede aufsteigende Kette $\Delta_1\subseteq\Delta_2\subseteq\ldots$ von Monoidealen wird letztlich stationär.
  $\Leftrightarrow$ Jede (nicht leere) Menge von Monoidealen besitzt ein maximales bzgl. Inklusion. Gemeint ist: Es gibt ein Ideal in dieser Menge, das in keinem anderen enthalten ist.
  - Beweis:
    - $1\Rightarrow 2$: Angenommen, $\Delta_1\subseteq\Delta_2\subseteq\ldots$ wird nicht stationär. Dann gibt es immer $\gamma_{i+1}\in\Delta_{i+1}\setminus\Delta_i$. Bilde Ideal aus $(\gamma_2,\ldots)$. Dieses ist nicht endlich erzeugt. Widerspruch.
    - $2\Rightarrow 3$: Wähle $\Delta_1\in$ Menge. Ist Δ_1 maximal, so fertig. Sonst gibt es $\Delta_2\supset\Delta_1$. Fahre induktiv fort. Erhalte eine Kette aus $\Delta_1\subset\Delta_2\subset\ldots$. Diese wird nach Voraussetzung letztendlich stationär, also $\Delta_n=\Delta_{n+1}=\ldots$. Dann ist Δ_n ein maximales Element.
    - $3\Rightarrow 1$: Δ Monoideal. Betrachte die Menge aller durch die Elemente von Δ endlich erzeugten Monoideale. Nach Voraussetzung gibt es in dieser Menge ein maximales $\tilde{\Delta}$. Es muss $\tilde{\Delta}=\Delta$ sein, sonst gäbe es $\gamma\in\Delta\setminus\tilde{\Delta}$, dass man dem endlichen Erzeugendensystem von $\tilde{\Delta}$ hinzufügen könnte, das wieder ein endliches Erzegendensystem eines weiteren Monoideals wäre, das größer als $\tilde{\Delta}$ wäre, was aber nicht geht, weil $\tilde{\Delta}$ maximal war. Widerspruch.
- Definition 'Noetherian': Γ erfüllt eben genannte Eigenschaften.
- $(\mathbb{N}^n,+)$ ist Noetherian.
- Definition 'monomialer Modul': Man kann ein Erzeugendensystem finden, das nur aus Monomen (Elemente aus $T^n\langle e_1,\ldots,e_r\rangle$) besteht; 'monomiales Ideal'
- Dickson's Lemma: $t_1,t_2,\ldots$ Sequenz von Termen in T^n. Dann sind ab hinter einem N alle Terme Vielfache der Terme $t_1,t_2,\ldots,t_N$, Das heißt, das **Monoideal** $(t_1,t_2,\ldots)$ wird erzeugt von $(t_1,t_2,\ldots,t_N)$. Das heißt jedes **monomiale Ideal** $(t_1,t_2,\ldots)\subseteq R[x_1,\ldots,x_n]$ ist endlich erzeugt.
  - Beweis:
    - Da $(\mathbb{N}^n,+)$ Noetherian ist und T^n via log isomorph zu $(\mathbb{N}^n,+)$ ist, folgt die Aussage über das *Monoideal*.
    - Da $(t_1,t_2,\ldots)\subseteq R[x_1,\ldots,x_n]$ ein *monomiales* Ideal ist, wird $(t_1,t_2,\ldots)$ auch durch $(t_1,t_2,\ldots,t_N)$ erzeugt.

- Darstellung von monomialen **Idealen** in der Ebene (2 Variablen)/ dem Raum (3 Variablen)
- Struktur-Theorem für monomiale Moduln: $M \subseteq P^r$ monomialer Modul, dann:
  - $M \cong \bigoplus_{i=1}^{r} I_i e_i$ mit monomialen Idealen I_i. (Beweis: klar)
  - M ist endlich erzeugt.:
    - Beweis: folgt aus '$M \cong \bigoplus_{i=1}^{r} I_i e_i$ mit monomialen Idealen I_i' und Dickson's Lemma angewendet auf die I_i-s
- Jede aufsteigende Kette $M_1 \subseteq M_2 \subseteq \ldots$ von monomialen Untermoduln wird letztlich stationär.:
  - Beweis:
    - Falls $M_1 \subset M_2 \subset \ldots$, wähle immer $t_{i+1} \in M_{i+1} \setminus M_i$. Dann ist $M := \langle t_2, t_3, \ldots \rangle \subseteq P^r$ im Widerspruch zum Struktur-Theorem nicht endlich erzeugt.
- $M \subseteq P^r$ monomialer Modul, dann:
  - Jeder Term aus M ist Vielfaches eines Terms aus dem monomialen Erzeugendensystem von M. (Beweis: klar)
  - Unter allen monomialen Erzeugendensystemen von M gibt es genau ein minimales.:
    - Beweis: Streiche aus einem Erzeugendensystem alle Vielfachen der Erzeuger.

1.4 Term Orderings

- Definition 'Relation'; 'vollständige Relation': Es gibt keine nicht vergleichbaren Elemente.
- Definition 'Monoid-Ordnung' (Γ Monoid):
  - $\gamma_1 \geq \gamma_1$ (reflexiv)
  - $\gamma_1 \geq \gamma_2 \wedge \gamma_2 \geq \gamma_1 \Rightarrow \gamma_1 = \gamma_2$ (antisymmetrisch)
  - $\gamma_1 \geq \gamma_2 \wedge \gamma_2 \geq \gamma_3 \Rightarrow \gamma_1 \geq \gamma_3$ (transitiv)
  - $\gamma_1 \geq \gamma_2 \Rightarrow \gamma_1 \circ \gamma_3 \geq \gamma_2 \circ \gamma_3$
- Definition 'Term-Ordnung' (Γ Monoid):
  - Monoid-Ordnung
  - $\gamma \geq 1 \forall \gamma \in \Gamma$
- Gilt die Kürzungsregel in Γ, dann:
  - $\gamma_1 \geq \gamma_2 \Leftarrow \gamma_1 \circ \gamma_3 \geq \gamma_2 \circ \gamma_3$:
    - Beweis: Annahme: $\gamma_1 < \gamma_2 \Rightarrow \gamma_1 \circ \gamma_3 \leq \gamma_2 \circ \gamma_3 \underset{\text{Kürzungsregel schließt '=' aus}}{\rightrightarrows} \gamma_1 \circ \gamma_3 < \gamma_2 \circ \gamma_3$
  - Γ ist unendlich.
    - Beweis: Es gilt $\gamma > 1$ xor $\gamma < 1$, also $\ldots > \gamma^2 > \gamma > 1$ xor $\ldots < \gamma^2 < \gamma < 1$.)
  - $\gamma^n \geq 1 \Leftrightarrow \gamma \geq 1$:
    - Beweis: Folgt mit Induktion aus $\gamma > 1$ xor $\gamma < 1$.
- Monoid-/ Term-Ordnungen zwischen T^n und $\mathbb{N}^n$ entsprechen sich wegen log.
- Definition 'Term-Ordnung Lex': $t_1 \geq_{\text{Lex}} t_2 :\Leftrightarrow$ erster Nicht-Null-Eintrag des Vektors $\log(t_1) - \log(t_2)$ ist positiv oder $t_1 = t_2$; 'Term-Ordnung DegLex': $t_1 \geq_{\text{DegLex}} t_2 :\Leftrightarrow \deg(t_1) > \deg(t_2) \vee \deg(t_1) = \deg(t_2) \wedge t_1 \geq_{\text{Lex}} t_2$; 'Term-Ordnung

DegRevLex': $t_1 \geq_{\text{DegRevLex}} t_2 :\Leftrightarrow \deg(t_1) > \deg(t_2)$ oder $\deg(t_1) = \deg(t_2)$ und der letzte Nicht-Null-Eintrag des Vektors $\log(t_1) - \log(t_2)$ ist negativ oder $t_1 = t_2$.

- Definition 'grad-kompatible Monoid-Ordnung auf T^n': $t_1 \geq t_2 \Rightarrow \deg(t_1) \geq \deg(t_2)$
- Defintion 'Eliminiation-Ordnung für $L := \{x_1, \ldots, x_j\}$': $t_1 \geq_{\text{Elim}(L)} t_2 :\Leftrightarrow \alpha_1 + \ldots + \alpha_j > \beta_1 + \ldots + \beta_j \vee \alpha_1 + \ldots + \alpha_j = \beta_1 + \ldots + \beta_j \wedge t_1 \geq_{\text{DegRevLex}} t_2$
- Definition 'durch eine Matrix representierte Ordnung': **Zeilen** linear unabhängig, $t_1 \geq_{\text{Ord}(V)} t_2 :\Leftrightarrow$ der erste Nicht-Null-Eintrag von $V \cdot (\log t_1 - \log t_2)$ ist positiv
- $\text{Ord}(V)$ ist eine Term-Ordnung. $\Leftrightarrow$ Der erste Nicht-Null-Eintrag jeder Spalte von V ist positiv.:
  - Beweis: alle $t \geq 1 \Leftrightarrow$ alle $x_i \geq 1 \Leftrightarrow V \cdot \left(\log x_i - \underbrace{\log 1}_{=0} \right) = V \cdot \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \vec{v}_i \underbrace{\geq}_{\text{erster Nicht-0-Eintrag}} 0$
- $V_{\text{Lex}} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$; $V_{\text{DegRevLex}} = \begin{pmatrix} 1 & \cdots & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & 0 & -1 \\ \vdots & \vdots & \ddots & \iddots & 0 \\ \vdots & 0 & \iddots & \ddots & \vdots \\ 0 & -1 & 0 & \cdots & 0 \end{pmatrix}$
- σ Monoid-Ordnung auf T^n, σ_i Einschränkung von σ auf $T_i^{n-1} := (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$, dann:
  - σ_i ist eine Monoid-Ordnung.
  - σ Term-Ordnung $\Rightarrow$ σ_i Term-Ordnung
  - V_{σ_i} erhält man, indem man aus V_σ die *i*-te Spalte streicht und dann die erste Zeile, die linear abhängig mit den Zeilen über ihr ist, ebenfalls streicht.
- Jede Monoid-Ordnung auf $\mathbb{N}^n$ hat eine eindeutige Erweiterung zu einer Monoid-Ordnung auf Z^n.:
  - Beweisidee: Zerpalte z in $z = n_1 - n_2$ und definiere $z \leq_{\sigma'} 0 :\Leftrightarrow n_1 \leq_\sigma n_2$
- $t_1 \geq_{\text{Ord}(V)} t_2 \Leftrightarrow V \cdot (\log t_1 - \log t_2) \geq_{\text{Lex}} 0$
- Definition 'Modul-Ordnung' ($(\Gamma, \circ)$ Monoid, $(\Sigma, *)$ Γ-Monomodul):
  - $s_1 \geq s_1$ (reflexiv)
  - $s_1 \geq s_2 \wedge s_2 \geq s_1 \Rightarrow s_1 = s_2$ (antisymmetrisch)
  - $s_1 \geq s_2 \wedge s_2 \geq s_3 \Rightarrow s_1 \geq s_3$ (transitiv)
  - $s_1 \geq s_2 \Rightarrow \gamma * s_1 \geq \gamma * s_2$
- Definition 'Modul-Term-Ordnung' ($(\Gamma, \circ)$ Monoid, $(\Sigma, *)$ Γ-Monomodul):
  - Modul-Ordnung
  - $\gamma * s \geq s \forall \gamma \in \Gamma, s \in \Sigma$
- $\Gamma = T^n$ und $\Sigma = T^n \langle e_1, \ldots, e_r \rangle$, dann ist die Modul-Term-Ordnung-Bedingung '$\gamma * s \geq s \forall \gamma \in \Gamma, s \in \Sigma$' äquivalent zu $te_i \geq e_i \forall t \in T^n$

- Definition ‘Modul-Term-Ordnung TOPos’ (TO ist Term-Ordnung auf T^n): $t_1e_i \geq_{\text{TOPos}} t_2e_j :\Leftrightarrow t_1 >_{\text{TO}} t_2 \vee t_1 = t_2 \wedge i \leq j$
- Definition ‘Modul-Term-Ordnung PosTO’ (TO ist Term-Ordnung auf T^n): $t_1e_i \geq_{\text{PosTO}} t_2e_j :\Leftrightarrow i < j \vee i = j \wedge t_1 >_{\text{TO}} t_2$
- Definition ‘zu einer Monoid-Ordnung ρ kompatible Modul-Ordnung σ’: $\gamma_1 \geq_\rho \gamma_2 \Rightarrow \gamma_1 * s \geq_\sigma \gamma_2 * s$
- Jede nicht-leere Untermenge von Σ hat ein minimales Element. $\Leftrightarrow$ Jede absteigende Kette $s_1 \geq s_2 \geq \ldots$ in Σ wird letztendlich stationär.
- Definition ‘Wohl-Ordnung’: Die eben genannten Bedingungen gelten.
- Wenn die Links-Kürzungsregel in Σ gilt, ist jede Wohl-Ordnung eine Modul-Term-Ordnung.
- fundamentale Eigenschaft von Term-Ordnungen: σ Modul-Ordnung auf $T^n\langle e_1,\ldots,e_r\rangle$. Dann: σ ist eine Modul-Term-Ordnung $\Leftrightarrow$ σ ist ein eine Wohl-Ordnung.

1.5 Leading Terms

- Definition ‘Leitterm LT’ ($m = \sum_{i=1}^{s} c_i t_i e_{\gamma_i}$): $t_1e_{\gamma_1}$; ‘Leitkoeffizient LC’: c_1 ; ‘monic’: $\text{LC}(m) = 1$; ‘Leitmonom LM’: $\text{LM}(m) = \text{LC}(m) \cdot \text{LT}(m)$
- Regeln fürs Rechnen mit Leittermen:
  - $\text{Supp}(m_1 + m_2) \subseteq \text{Supp}(m_1) \cup \text{Supp}(m_2)$; $\text{LT}(m_1 + m_2) \leq \max\{\text{LT}(m_1), \text{LT}(m_2)\}$
  - $\text{LT}(m_1 + m_2) = \max\{\text{LT}(m_1), \text{LT}(m_2)\}$, falls $\text{LT}(m_1) \neq \text{LT}(m_2) \vee \text{LC}(m_1) + \text{LC}(m_2) \neq 0$
  - $\text{LT}(tm) = t \cdot \text{LT}(m)$
  - R Integritätsbereich, dann: $t \in \text{Supp}(f)$, für den $t \cdot \text{LT}(m)$ maximal ist $\Rightarrow$ $\text{LT}(fm) = t \cdot \text{LT}(m)$
  - R Integritätsbereich, σ kompatibel zu ρ, dann: $\text{LT}(fm) = \text{LT}_\rho(f) \cdot \text{LT}_\sigma(m)$
- Definition ‘Leitterm-Modul eines Moduls $\text{LT}(M)$’: $\text{LT}(M) = \langle \text{LT}(m) | m \in M \setminus \{0\} \rangle$; ‘Leitterm-Ideal’; ‘Leitterm-Monomodul $\text{LT}\{M\}$’: $\text{LT}\{M\} := \{\text{LT}(m) | m \in M \setminus \{0\}\}$ (ist Monomodul)
- $M = (m_1,\ldots,m_s) \Rightarrow \langle \text{LT}(m_1),\ldots,\text{LT}(m_s) \rangle \subseteq \text{LT}(M)$:
- Beispiel für $\langle \text{LT}(m_1),\ldots,\text{LT}(m_s) \rangle \subset \text{LT}(M)$: $M := \langle x^2 - 1, xy - 1 \rangle \Rightarrow y(x^2 - 1) - x(xy - 1) = x - y \in M \Rightarrow x \in \text{LT}(M)$, aber $x \notin \langle x^2, xy \rangle$
- $te_i \in \text{LT}(M) \Rightarrow \exists m \in M : te_i = \text{LT}(m)$
  - Beweis: $te_i \in \text{LT}(M) \Rightarrow te_i \in \text{LT}\{M\} \Rightarrow \exists t' \in T^n, m' \in M : te_i = t' \cdot \text{LT}(m') = \text{LT}\left(\underbrace{t'm'}_{=:m \in M} \right)$
- $\exists m_1,\ldots,m_s \in M : \text{LT}(M) = \langle \text{LT}(m_1),\ldots,\text{LT}(m_s) \rangle$:
  - Beweis:
    - $\text{LT}(M)$ ist monomialer Modul.
    - Nach Dickson’s Lemma gibt es ein endliches Erzeugendensystem $(t_1e_{i_1},\ldots,t_se_{i_s})$ für $\text{LT}(M)$.
    - Laut ‘$t_je_{i_j} \in \text{LT}(M) \Rightarrow \exists m_j \in M : t_je_{i_j} = \text{LT}(m_j)$’ gibt es die gesuchten m_j-s.

- Macaulay's Basis Theorem: $B := T^n\langle e_1,\ldots,e_r\rangle \setminus \mathrm{LT}\{M\}$ ist eine Basis des ***K*-Vektorraums** P^r / M.
- $\sigma = \mathrm{Lex} \Leftrightarrow (f \in P, \mathrm{LT}_\sigma(f) \in R[x_i,\ldots,x_n] \Rightarrow f \in R[x_i,\ldots,x_n])$
- $\sigma = \mathrm{RevLex} \Leftrightarrow (f \in P, \mathrm{LT}(f) \in (x_i,\ldots,x_n) \Rightarrow f \in (x_i,\ldots,x_n))$
- $\sigma = \mathrm{DegRevLex} \Leftrightarrow (f \in P \text{ und homogen}, \mathrm{LT}(f) \in (x_i,\ldots,x_n) \Rightarrow f \in (x_i,\ldots,x_n))$

1.6 The Division Algorithm

- Divisionsalgorithmus bei mehreren Variablen
- Das Ergebnis hängt von der Term-Ordnung und der Reihenfolge der g_i ab.
- Rückgabe des Algorithmus's: $m = q_1 g_1 + \ldots + q_s g_s + p$ mit den Eigenschaften:
  - Kein Element in $\mathrm{Supp}(p)$ ist enthalten in $\langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s)\rangle$.
  - $\mathrm{LT}(q_i g_i) \le \mathrm{LT}(m)$
  - $t \in \mathrm{Supp}(q_i)$, dann $t \cdot \mathrm{LT}(g_i) \notin \langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_{i-1})\rangle$
- Mit dem Divisionalgorithmus ist es nicht immer möglich zu entscheiden, ob $m \in \langle g_1,\ldots,g_s\rangle$.
- Es lässt sich lediglich **ein Element** der Restklasse von m modulo $\langle g_1,\ldots,g_s\rangle$ berechnen (dieses könnte z. B. in der Restklasse von 0 liegen, ohne dass man es ihm ansieht).
- Außerdem lassen sich nicht mit jedem Satz $g_1,\ldots,g_s$ die Elemente in $P^r/(g_1,\ldots,g_s)$ als Linearkombination von Termen aus $T^n \setminus (\mathrm{LT}(g_1)\ldots,\mathrm{LT}(g_s))$ ausdrücken, wie es laut Macaulay's Basis Theorem möglich ist (mit günstigen $g_1,\ldots,g_s$).
- Definition 'normaler Rest $\mathrm{NR}_{\sigma,G}(m)$': das p aus $m = q_1 g_1 + \ldots + q_s g_s + p$

1.7 Gradings

- Definition 'Γ-graduierter Ring R':
  - $R = \bigoplus_{\gamma\in\Gamma} R_\gamma$
  - $R_\gamma \cdot R_{\gamma'} \subseteq R_{\gamma+\gamma'} \forall \gamma,\gamma' \in \Gamma$
- Definition 'homogenes Element r vom Grad γ': r liegt in R_γ; 'deg': $\deg(r) = \gamma$; 'homogene Komponente r_γ vom Grad γ von r': $r = \sum_{\gamma\in\Gamma} r_\gamma$
- Die Dekomposition von r in seine homogenen Komponenten r_γ ist eindeutig. (Wegen der direkten Summe in $R = \bigoplus_{\gamma\in\Gamma} R_\gamma$.)
- Die Kürzungsregel gilt in Γ, dann:
  - R_0 ist Unterring von R.
  - Jedes R_γ ist R_0-Modul.
- Definition 'Standard-Graduierung für den Polynomring': $P_d := \{f \in P \mid \deg(t) = d \forall t \in \mathrm{Supp}(f)\}$; 'homogenes Polynom vom Grad d': Elemente aus P_d; Definition '$\mathbb{N}^n$-Graduierung für den Polynomring': $P_{(\alpha_1,\ldots,\alpha_n)} := R x_1^{\alpha_1} \ldots x_n^{\alpha_n}$

- Definition 'Σ-graduierter R-Modul M':
  - $M = \bigoplus_{s\in\Sigma} M_s$
  - $R_\gamma \cdot M_s \subseteq M_{\gamma * s}$
- Die Kürzungsregel gilt in Γ, dann: jedes M_s ist R_0-Modul
- Definition 'Gradverschiebung' $M(\gamma)_s := M_{\gamma * s}$; '$M(\gamma)$': $M(\gamma) := \bigoplus_{s\in\Sigma} M(\gamma)_s$; '$\Gamma$-graduiert-freier R-Modul F': $F := \begin{pmatrix} R(\gamma_1) \\ \vdots \\ R(\gamma_r) \end{pmatrix} = \bigoplus_{i\in I:=\{1,\ldots,r\}} R(\gamma_i)$
- Definition 'Homomorphismus Γ-graduierter Ringe (φ,ψ)': $\varphi(R_\gamma) \subseteq S_{\psi(\gamma)} \forall \gamma \in \Gamma$; 'Homomorphismus Σ-graduierter R-Moduln $\lambda : M \to N$': $\lambda(M_s) \subseteq N_s \forall s \in \Sigma$
- Definition 'Σ-graduierter R-Untermodul N von M': $N = \bigoplus_{s\in\Sigma} (N \cap M_s)$; '$\Gamma$-homogenes Ideal I von R': $I = \bigoplus_{\gamma\in\Gamma} (I \cap R_\gamma)$
- N ein Σ-graduierter R-Untermodul von M, $(M/N)_s := M_s / N_s$, dann: M/N ein Σ-graduierter R-Modul
- N ein Σ-graduierter R-Untermodul von M, $N_s := N \cap M_s$, dann:
  $N := \bigoplus_{s\in\Sigma} N_s$
  $\Leftrightarrow \left(\underbrace{n}_{\in N} = \sum_{s\in\Sigma} \underbrace{n_s}_{\in M} \text{ (Zerlegung in homogene Komponenten von } n \text{ in } M, \text{ nicht in } N) \Rightarrow n_s \in N \forall s \in \Sigma \right)$
  $\Leftrightarrow \exists$ Erzeugendensystem von N, das nur aus homogenen Elementen besteht.

  - Beweis:
    - $1 \Rightarrow 2$: Die Zerlegung von n in M ist dieselbe wie in N.
    - $2 \Rightarrow 3$: Zerlege alle Erzeuger eines beliebigen Erzeugendensystems in ihre homogenen Komponenten. Diese liegen nach Voraussetzung in N und bilden alle zusammen das gesuchte homogene Erzeugendensystem.
    - $3 \Rightarrow 1$: $n = \sum r_\beta n_\beta$ Darstellung von n in der Basis mit Faktoren r_β aus R (z. B. dem Polynomring). Zerlege die r_β-s in homogene Komponenten $r_{\beta,\gamma}$, bilde $r_{\beta,\gamma} n_\beta \in N_s$ für ein s und sortiere die verschiedenen $r_{\beta,\gamma} n_\beta$ nach den s.
- Rechts-Kürzungsregel gilt in Σ, N ein Σ-graduierter R-Untermodul von M, $(n_\beta \in B)$ homogenes Erzeugendensystem von N, dann: Jedes Element $n \in N_s$ hat eine eindeutige Darstellung $n = \sum_{\beta\in B} r_\beta n_\beta$ mit homogenen Elementen $r_\beta \in R$, so dass $\deg(r_\beta) * \deg(n_\beta) = s \forall \beta \in B$.
- I homogenes, echtes Ideal von R, dann:
  I ist Primideal ($h = fg \in I; f, g \in R \Rightarrow f \in P \vee g \in P$).
  $\Leftrightarrow h = fg \in I; f, g \in R$ homogen $\Rightarrow f \in P \vee g \in P$
- $R_+ := \bigoplus_{\gamma>0} R_\gamma$ ist ein homogenes Ideal von R.
- graduierte Version von Nakayama's Lemma: $M_1 \subseteq M_2 \subseteq M_1 + R_+ \cdot M_2 \Rightarrow M_1 = M_2$:
  - Beweis:
    - nur noch zu zeigen: $M_2 \subseteq M_1$

- Angenommen, nicht, dann gibt es ein homogenes $m \in M_2 \setminus M_1$ mit minimalem Grad.
- wegen $M_2 \subseteq M_1 + R_+ \cdot M_2$: $m = \underbrace{m'}_{\in M_1} + \sum_{i=1}^{t} \underbrace{f_i}_{\in R_+} \underbrace{g_i}_{\in M_2}$.
- Wegen $\deg(f_i) > 0$ und $\deg(m) = \deg(f_i) * \deg(g_i)$ ist $\deg(g_i) < \deg(m)$. Nach Wahl von m sind also $g_i \in M_1$.
- Also $m = \underbrace{m'}_{\in M_1} + \sum_{i=1}^{t} \underbrace{\underbrace{f_i}_{\in R_+} \underbrace{g_i}_{\in M_1}}_{\in M_1} \in M_1$ und nicht $m \in M_2 \setminus M_1$. Widerspruch.

- $(m_1,\ldots,m_s)$ (m_i-s homogene Elemente) erzeugt M. $\Leftrightarrow (\overline{m}_1,\ldots,\overline{m}_s)$ erzeugt $M/R_+ \cdot M$.:
  - Beweis:
    - '$\Rightarrow$': klar
    - '$\Leftarrow$':
      - Sei $N := (m_1,\ldots,m_s) \subseteq M$.
      - nach Voraussetzung $N \cong M/R_+ \cdot M \Rightarrow N + R_+ \cdot M = M \Rightarrow N + R_+ \cdot M \supseteq M$
      - mit Nakayama's Lemma $N = M$
- R_0 Körper, dann: Jedes homogene Erzeugendensystem von M enthält ein minimales.:
  - Beweis:
    - Sei $M = (m_1,\ldots,m_s)$. Gehe über zu $\overline{M} = M/R_+ \cdot M$. Dann: $\overline{M} = (\overline{m}_1,\ldots,\overline{m}_s)$.
    - Da $R_0 \cong R/R_+$ ein Körper ist und $\overline{M} = M/R_+ \cdot M$ ein R_0-Modul ist, ist $\overline{M}$ sogar ein Vektorraum.
    - Vektorräume besitzen minimale Erzeugendensysteme, nämlich Basen. Streiche also $(\overline{m}_1,\ldots,\overline{m}_s)$ zu einer Basis zusammen, o. B. d. A. $(\overline{m}_1,\ldots,\overline{m}_r)$ mit $r \le s$.
    - dann: $M = (m_1,\ldots,m_r)$

2.1 Special Generation

- spezielle Erzeugung von Untermoduln: M P-Untermodul von P^r, $g_1,\ldots,g_s \in P^r \setminus \{0\}$ ($(g_1,\ldots,g_s)$ sind ein spezielles Erzeugendensystem von M, wenn die Bedingungen erfüllt sind), dann:

  $$A_1 : \forall m \in M \setminus \{0\} \exists f_1,\ldots,f_s \in P : m = \sum_{i=1}^{s} f_i g_i \wedge \mathrm{LT}(m) \ge \mathrm{LT}(f_i g_i)$$

  $$\Leftrightarrow A_2 : \forall m \in M \setminus \{0\} \exists f_1,\ldots,f_s \in P : m = \sum_{i=1}^{s} f_i g_i \wedge \mathrm{LT}(m) = \max\{\mathrm{LT}(f_i g_i)\}$$

  - Beweis: klar
- Erzeugung von Leitterm-Moduln: M P-Untermodul von P^r, $g_1,\ldots,g_s \in P^r \setminus \{0\}$, dann:

  $$B_1 : (\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s)) \text{ erzeugt } \mathrm{LT}\{M\}.$$

  $$\Leftrightarrow B_2 : (\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s)) \text{ erzeugt } \mathrm{LT}(M).$$

  - Beweis: klar
- M P-Untermodul von P^r, $g_1,\ldots,g_s \in P^r \setminus \{0\}$, dann: $A_1 \Leftrightarrow A_2 \Leftrightarrow B_1 \Leftrightarrow B_2$
  - Beweis:
    - $A_2 \Rightarrow B_1$: Für alle m ist $\mathrm{LT}(m) = \max\{\mathrm{LT}(f_i g_i)\} \Rightarrow \mathrm{LT}(m) = \mathrm{LT}(f_j g_j) = \mathrm{LT}(f_j) \cdot \mathrm{LT}(g_j)$

für ein j und somit $\mathrm{LT}(m) \in (\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s))$

- $B_1 \Rightarrow A_1$:
  - Angenommen, es gibt m-s, die nicht dargestellt werden können. Wähle ein kleinstes.
  - Sei $\mathrm{LT}(m) = t \cdot \mathrm{LT}(g_j)$. Wegen der Wahl von m hat $m' = m - tg_j$ eine Darstellung.
  - Dann aber auch $m = m' + tg_j$. Widerspruch.

2.2 Rewrite Rules

- Definition 'm_1 reduziert sich auf m_2 in einem Schritt mit der Ersetzungsregel g_i ($m_1 \overset{g_i}{\to} m_2$): $m_2 = m_1 - ctg_i \wedge t \cdot \mathrm{LT}(g_i) \notin \mathrm{Supp}(m_2)$; '$m_1 \overset{G}{\to} m_2$': m_1 reduziert sich auf m_2 in mehreren Schritten beliebigen g_i-s; 'irreduzibel bzgl. $\overset{G}{\to}$': nicht mehr reduzierbar
- Eigenschaften von Ersetzungs-Relationen: σ **Term**-Ordnung
  - $m_1 \overset{G}{\to} m_2 \wedge m_2 \overset{G}{\to} m_1 \Rightarrow m_1 = m_2$
    - Beweis: klar
  - $m_1 \overset{G}{\to} m_2 \Rightarrow tm_1 \overset{G}{\to} tm_2$
    - Beweis: klar
  - $m_1 \overset{G}{\to} m_2 \overset{G}{\to} \ldots$ wird letztendlich stationär
    - Beweis: Durch das Reduzieren wird jeweils ein Term durch zwar u. U. mehrere andere, aber echt kleinere ersetzt.
  - $m_1 \overset{g_i}{\to} m_2, m_3$ beliebig $\Rightarrow \exists m_4 : m_1 + m_3 \overset{G}{\to} m_4 \wedge m_2 + m_3 \overset{G}{\to} m_4$
    - Beweisidee: $m_4 := \underbrace{m_1}_{=m_2+ct\mathrm{LT}(g_i)} + m_3 - (c+c')t\mathrm{LT}(g_i) = m_2 + m_3 - c't\mathrm{LT}(g_i)$
  - $m_1 \overset{G}{\leftrightarrow} m_2 \wedge m_3 \overset{G}{\leftrightarrow} m_4 \Rightarrow m_1 + m_3 \overset{G}{\leftrightarrow} m_2 + m_4$:
    - Beweis: klar
  - $m_1 \overset{G}{\leftrightarrow} m_2 \Rightarrow fm_1 \overset{G}{\leftrightarrow} fm_2$:
    - Beweis: folgt aus '$m_1 \overset{G}{\to} m_2 \Rightarrow tm_1 \overset{G}{\to} tm_2$'
  - $m \overset{G}{\leftrightarrow} 0 \Leftrightarrow m \in \langle g_1,\ldots,g_s \rangle$:
    - Beweis: $m \overset{G}{\leftrightarrow} 0 \Leftrightarrow m - \sum f_i g_i = 0 \Leftrightarrow m = \sum f_i g_i \Leftrightarrow m \in \langle g_1,\ldots,g_s \rangle$
  - $m_1 \overset{G}{\leftrightarrow} m_2 \Leftrightarrow m_1 - m_2 \in \langle g_1,\ldots,g_s \rangle$
    - Beweis: Folgt aus '$m \overset{G}{\leftrightarrow} 0 \Leftrightarrow m \in \langle g_1,\ldots,g_s \rangle$'.
- $M := \langle g_1,\ldots,g_s \rangle$ P-Untermodul von P^r, dann:

$C_1 : m \xrightarrow{G} 0 \Leftrightarrow m \in M$

$\Leftrightarrow C_2 : m \in M$ irreduzibel bzgl. $\xrightarrow{G} \Rightarrow m = 0$

$\Leftrightarrow C_3 : m_1 \in P^r \Rightarrow \exists 1 m_2 \in P^r : m_1 \xrightarrow{G} m_2 \wedge m_2$ irreduzibel bzgl. $\xrightarrow{G}$

$\Leftrightarrow C_4 : m_1 \xrightarrow{G} m_2 \wedge m_1 \xrightarrow{G} m_3 \Rightarrow \exists m_4 : m_2 \xrightarrow{G} m_4 \wedge m_3 \xrightarrow{G} m_4$

- Beweis:
  - $1 \Rightarrow 2$: $m \in M \underbrace{\Rightarrow}_{C_1} m \xrightarrow{G} 0 \Rightarrow m = 0$, weil m irreduzibel ist.
  - $2 \Rightarrow 3$: Annahme: $m_1 \xrightarrow{G} m_2 \wedge m_1 \xrightarrow{G} \tilde{m}_2 \Rightarrow m_2 - \tilde{m}_2 \in M$ und irreduzibel $\underbrace{\Rightarrow}_{C_2} m_2 - \tilde{m}_2 = 0 \Rightarrow m_2 = \tilde{m}_2$
  - $3 \Rightarrow 4$: $\exists m_2', m_3'$ irreduzibel : $m_2 \xrightarrow{G} m_2' \wedge m_3 \xrightarrow{G} m_3' \Rightarrow m_1 \xrightarrow{G} m_2' \wedge m_1 \xrightarrow{G} m_3' \underbrace{\Rightarrow}_{C_3} m_2' = m_3' =: m_4$
  - $4 \Rightarrow 1$: siehe ‘University; Computational Commutative Algebra 1; Lecture Notes’
- Definition ‘confluent’: C_4 ist erfüllt.
- $m \xrightarrow{G} 0$, dann:
  - $\mathrm{LT}(m) = t \cdot \mathrm{LT}(g_\alpha)$ für ein $g_\alpha \in \{g_1, \ldots, g_s\}$:
    - Beweis: Weil $\mathrm{LT}(m)$ in irgendeinem Reduktionsschritt verschwinden muss.
  - $\exists f_i' : m - \frac{\mathrm{LC}(m)}{\mathrm{LC}(g_\alpha)} t g_\alpha = \sum_{i=1}^{s} f_i' g_i \wedge \mathrm{LT}(m) > \mathrm{LT}(f_i' g_i) \forall i$
    - Beweis: Sammle die ct-s zu jedem g_i aus den Reduktionsschritten.
  - $\exists f_i : m = \sum_{i=1}^{s} f_i g_i \wedge \mathrm{LT}(m) = \max\{\mathrm{LT}(f_i g_i)\}$
    - Beweis: wegen ‘$m = \sum_{i=1}^{s} f_i' g_i + \frac{\mathrm{LC}(m)}{\mathrm{LC}(g_\alpha)} t g_\alpha$’
- $M := \langle g_1, \ldots, g_s \rangle$ P-Untermodul von P^r, dann: $A_1 \Leftrightarrow A_2 \Leftrightarrow B_1 \Leftrightarrow B_2 \Leftrightarrow C_1 \Leftrightarrow C_2 \Leftrightarrow C_3 \Leftrightarrow C_4$
  - Beweis:
    - $A_2 \Rightarrow C_2$:
      - Angenommen, es gibt $\underbrace{m}_{\in M} \neq 0$ irreduzibel.
      - nach A_2: $m = \sum_{i=1}^{s} f_i g_i \wedge \mathrm{LT}(m) = \max\{\mathrm{LT}(f_i g_i)\}$. Sei t der Term mit $\mathrm{LT}(m) = \max\{\mathrm{LT}(f_i g_i)\} = t \cdot \mathrm{LT}(g_i)$
      - Dies bedeutet aber, dass sich m mit g_i reduzieren lässt. Widerspruch.
    - $C_1 \Rightarrow A_2$: bereits gezeigt in ‘$m \xrightarrow{G} 0 \Rightarrow \exists f_i : m = \sum_{i=1}^{s} f_i g_i \wedge \mathrm{LT}(m) = \max\{\mathrm{LT}(f_i g_i)\}$’

2.3 Syzygies

- Definition ‘Syzygie von $G := (g_1,\ldots,g_s)$’ $(g_i \in M)$: $(f_1,\ldots,f_s): \sum_{i=1}^{s} f_i g_i = \vec{0}$ $(f_i \in R)$; ‘Syzygien-Modul von G $\mathrm{Syz}(G)$’: Menge aller Syzygien von G
- $\lambda: \begin{matrix} P^s \to M \\ \varepsilon_i \mapsto g_i \end{matrix}$, dann: $\mathrm{Syz}(G) = \ker(\lambda)$
- Definition ‘exakte Sequenz’: $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$ mit $\mathrm{im}(f_1) = \ker(f_2)$
- $0 \to M \to P^r \to P^r / M \to 0$ ergibt nach Einbau von λ $0 \to \mathrm{Syz}(G) \to P^s \xrightarrow{\lambda} P^r \to P^r / M \to 0$
- $N := (\mathrm{LM}(g_1),\ldots,\mathrm{LM}(g_s))$, $\Lambda: \begin{matrix} P^s \to N \\ \varepsilon_i \mapsto \mathrm{LM}(g_i) \end{matrix}$, dann: $\mathrm{Syz}(\mathrm{LM}(G)) = \ker(\Lambda)$
- $0 \to \mathrm{Syz}(\mathrm{LM}(G)) \to P^s \xrightarrow{\Lambda} P^r \to P^r / M \to 0$
- $(P^s)_{te_i} := \left\{ \sum_{j=1}^{s} c_j t_j \varepsilon_j \in P^s \,\middle|\, t_j\, \mathrm{LT}(g_j) = te_i \right\}$, dann:
  - P^s wird zu einem $T^n\langle e_1,\ldots,e_r\rangle$-graduierten Modul über dem T^n-graduierten Ring P, denn $P^s = \bigoplus_{te_i \in T^n\langle e_1,\ldots,e_r\rangle} (P^s)_{te_i}$
  - Λ ist ein Homomorphismus $T^n\langle e_1,\ldots,e_r\rangle$-graduierter P-Moduln (d. h. $\Lambda((P^s)_{te_i}) \subseteq (P^r)_{te_i}$)
  - $0 \to \mathrm{Syz}(\mathrm{LM}(G)) \to P^s \xrightarrow{\Lambda} P^r \to P^r / M \to 0$ besteht aus Homomorphismen $T^n\langle e_1,\ldots,e_r\rangle$-graduierter Moduln.
- Definition ‘σ-Grad von m $\deg_\sigma(m)$’ ($m = \sum_{te_i \in T^n\langle e_1,\ldots,e_r\rangle} m_{te_i}$ Dekomposition von m in seine homogenen Komponenten): $\deg_\sigma(m) := \max\{te_i\}$; ‘$\sigma$-Leitform von m $\mathrm{LF}_\sigma(m)$’: $\mathrm{LF}_\sigma(m) := m_{\deg_\sigma(m)}$
- Definition ‘$\deg_{\sigma,G}(m)$’ ($(P^s)_{te_i} := \left\{ \sum_{j=1}^{s} c_j t_j \varepsilon_j \in P^s \,\middle|\, t_j\, \mathrm{LT}(g_j) = te_i \right\}$, s. o.); ‘$\mathrm{LF}_{\sigma,G}(m)$’
- $m = \sum_{j=1}^{s} f_j \varepsilon_j$, dann:
  - $\deg_{\sigma,G}(m) = \max\{\mathrm{LT}(f_j g_j)\}$
  - $\mathrm{LF}_{\sigma,G}(m) = \sum_{j=1}^{s} \bar{f}_j \varepsilon_j$, wobei
    $$\bar{f}_j = \begin{cases} 0, \text{falls } \mathrm{LT}(f_j g_j) < \deg_{\sigma,G}(m) \\ \underbrace{c_j t_j}_{\triangleq \mathrm{LM}(f_j)}, \text{falls } \mathrm{LT}(f_j g_j) = \deg_{\sigma,G}(m) \wedge \mathrm{LM}(f_j g_j) = \underbrace{c_j t_j}_{\triangleq \mathrm{LM}(f_j)}\, \mathrm{LM}(g_j) \end{cases}$$
- fundamentales Diagramm:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{Syz}(G) & \to & P^s & \xrightarrow{\lambda} & P^r & \to & P^r / M \to 0 \\ & & & & \downarrow \mathrm{LF} & & \downarrow \mathrm{LM} & & \\ 0 & \to & \mathrm{Syz}(\mathrm{LM}(G)) & \to & P^s & \xrightarrow{\Lambda} & P^r & \to & P^r / N \to 0 \end{array}$$

- bzgl. der Kommutativität des Diagramms:
  - $m \in P^s \setminus \mathrm{Syz}(G)$, dann:
    - $\mathrm{LT}(\lambda(m)) \leq \deg_{\sigma,G}(m)$
    - $\mathrm{LF}(m) \in \mathrm{Syz}(\mathrm{LM}(G)) \Leftrightarrow \mathrm{LT}(\lambda(m)) < \deg_{\sigma,G}(m)$
    - $\Lambda(\mathrm{LF}(m)) = \mathrm{LM}(\lambda(m)) \Leftrightarrow \mathrm{LT}(\lambda(m)) = \deg_{\sigma,G}(m)$
  - $m \in \mathrm{Syz}(G)$, dann: $\mathrm{LF}(m) \in \mathrm{Syz}(\mathrm{LM}(G))$ und $\mathrm{LF}_{|\mathrm{Syz}(G)} : \mathrm{Syz}(G) \to \mathrm{Syz}(\mathrm{LM}(G))$
  - Beweis: klar (siehe 'University; Computational Commutative Algebra 1; Lecture Notes')
- Syzygien von Elementen von monomialen Modulen: $\mathrm{LM}(g_j) = c_j t_j e_{\gamma_j}$, $t_{ij} := \frac{\mathrm{kgV}(t_i, t_j)}{t_i} = \frac{t_j}{\mathrm{ggT}(t_i, t_j)}$:
  - Für $i < j \wedge \gamma_i = \gamma_j$ ist $\sigma_{ij} := \frac{1}{c_i} t_{ij} \varepsilon_i - \frac{1}{c_j} t_{ji} \varepsilon_j$ eine Syzygie von $\mathrm{LM}(G)$ und homogen vom σ-Grad $\deg_{\sigma,G}(\sigma_{ij}) = \mathrm{kgV}(t_i, t_j) e_{\gamma_i}$
  - $\mathrm{Syz}(\mathrm{LM}(G)) = \left\langle \sigma_{ij} \middle| 1 \leq i < j \leq s \wedge \gamma_i = \gamma_j \right\rangle$, also endlich erzeugt und ein $T^n\langle e_1, \ldots, e_r \rangle$-graduierter Untermodul von P^s
- $\gamma_i \neq \gamma_j \forall 1 \leq i < j \leq s \Rightarrow$ Nur $(0, \ldots, 0)$ ist Syzygie.
  - Beweis: klar
- Definition 'Liftung $m \in P^s$ eines Elements $\overline{m} \in P^s$': $\mathrm{LF}(m) = \overline{m}$
- D-Bedingungen:

  D_1: Jedes homogene Element aus $\mathrm{Syz}(\mathrm{LM}(G))$ hat eine Liftung in $\mathrm{Syz}(G)$.

  $\Leftrightarrow D_2$: Es gibt ein homogenes Erzeugendensystem von $\mathrm{Syz}(\mathrm{LM}(G))$, das nur aus Elementen besteht, die Liftungen in $\mathrm{Syz}(G)$ haben.

  $\Leftrightarrow D_3$: Es gibt ein endliches, homogenes Erzeugendensystem von $\mathrm{Syz}(\mathrm{LM}(G))$, das nur aus Elementen besteht, die Liftungen in $\mathrm{Syz}(G)$ haben.
  - Beweis:
    - $1 \Rightarrow 3$:
      - Nach '$\mathrm{Syz}(\mathrm{LM}(G)) = \left\langle \sigma_{ij} \middle| 1 \leq i < j \leq s \wedge \gamma_i = \gamma_j \right\rangle$' gibt es ein endliches Erzeugendensystem von $\mathrm{Syz}(\mathrm{LM}(G))$.
      - Nach Voraussetzung (D_1) haben diese Erzeuger Liftungen in $\mathrm{Syz}(G)$.
    - $3 \Rightarrow 2$: trivial
    - $2 \Rightarrow 1$:
      - Stelle das homogene Element aus $\mathrm{Syz}(\mathrm{LM}(G))$ als Linearkombination der nach D_2 existierenden Erzeuger dar.
      - Ersetze in der Linearkombination die Erzeuger durch ihre Liftungen in $\mathrm{Syz}(G)$.
      - Dies ist die gesuchte Liftung des homogenen Elements.
- $(\overline{m}_1, \ldots, \overline{m}_t)$ homogenes Erzeugendensystem von $\mathrm{Syz}(\mathrm{LM}(G))$ und $m_1, \ldots, m_t \in \mathrm{Syz}(G)$ die Liftungen (d. h. $\mathrm{LF}(m_i) = \overline{m}_i$), dann: $(m_1, \ldots, m_t)$ Erzeugendensystem von $\mathrm{Syz}(G)$
  - Beweis:
    - Angenommen, es gibt m-s in $\mathrm{Syz}(G)$, die nicht als Linearkombination der m_i-s dargestellt werden können. Wähle ein kleinstes m.

- Weil $(\overline{m}_1,\ldots,\overline{m}_t)$ $\mathrm{Syz}(\mathrm{LM}(G))$ erzeugt und $\mathrm{LF}(m)\in \mathrm{Syz}(\mathrm{LM}(G))$, besitzt $\mathrm{LF}(m)$ eine Darstellung $\mathrm{LF}(m)=\sum c_j t_j \overline{m}_{i_j}$.
- Dann ist $m' := m-\sum c_j t_j m_{i_j}$ kleiner als m und kann somit mit $(m_1,\ldots,m_t)$ dargestellt werden.
- Dann aber auch $m := m'+\sum c_j t_j m_{i_j}$. Widerspruch.

- $M := \langle g_1,\ldots,g_s\rangle$ P-Untermodul von P^r, dann:
  $A_1 \Leftrightarrow A_2 \Leftrightarrow B_1 \Leftrightarrow B_2 \Leftrightarrow C_1 \Leftrightarrow C_2 \Leftrightarrow C_3 \Leftrightarrow C_4 \Leftrightarrow D_1 \Leftrightarrow D_2 \Leftrightarrow D_3$
  - Beweis:
    - $A_2 \Rightarrow D_1$: siehe 'University; Computational Commutative Algebra 1; Lecture Notes'
    - $D_1 \Rightarrow A_2$: siehe 'University; Computational Commutative Algebra 1; Lecture Notes'

2.4 Gröbner Bases of Ideals and Modules

- Charakterisierung von Gröbner-Basen: $M := \langle g_1,\ldots,g_s\rangle$ P-Untermodul von P^r, dann:
  $A_1 \Leftrightarrow A_2 \Leftrightarrow B_1 \Leftrightarrow B_2 \Leftrightarrow C_1 \Leftrightarrow C_2 \Leftrightarrow C_3 \Leftrightarrow C_4 \Leftrightarrow D_1 \Leftrightarrow D_2 \Leftrightarrow D_3$
- Definition 'σ-Gröbner-Basis $(g_1,\ldots,g_s)$': $(g_1,\ldots,g_s)$ erfüllt $A_1,\ldots,D_3$

2.4.1 Existenz von Gröbner-Basen

- $g_1,\ldots,g_s \in \underbrace{M}_{\text{wichtig!}} \wedge \mathrm{LT}(M)=\langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s)\rangle \Rightarrow M=\langle g_1,\ldots,g_s\rangle \wedge (g_1,\ldots,g_s)$ ist σ-Gröbner-Basis.
  - Beweis:
    - Annahme: Es gibt $m\in M\setminus\langle g_1,\ldots,g_s\rangle$. Wähle ein minimales aus.
    - Dann ist wegen $\mathrm{LT}(M)=\langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s)\rangle$ $\mathrm{LM}(m)=ct\,\mathrm{LT}(g_i)$
    - Nach Wahl von m ist $m' := m-ctg_i \in \langle g_1,\ldots,g_s\rangle$.
    - Dann aber auch $m=m'+ctg_i$. Widerspruch.
- Es gibt immer eine σ-Gröbner-Basis.
  - Beweis: Folgt aus eben Gezeigtem und Proposition 1.5.6.b $(\exists m_1,\ldots,m_s\in M:\mathrm{LT}(M)=\langle \mathrm{LT}(m_1),\ldots,\mathrm{LT}(m_s)\rangle)$.
- Definition 'Noetherian Ring/ Modul'. Jede aufsteigende Kette von Idealen/ Untermoduln wird letztendlich stationär.
- R Ring, M R-Modul, dann:
  Jeder Untermodul in M ist endlich erzeugt.
  $\Leftrightarrow$ Jede aufsteigende Kette $N_1\subseteq N_2\subseteq\ldots$ von Untermoduln wird letztlich stationär.
  $\Leftrightarrow$ Jede (nicht leere) Menge von Untermoduln besitzt ein maximales bzgl. Inklusion.
- Hilbert's Basis Theorem:
  - Buch-Variante: Jeder endlich erzeugte Modul M über einer endlich erzeugten K-Algebra ist Noetherian. Insbesondere ist $K[x_1,\ldots,x_n]$ ein Noetherian Ring.
    - Beweisidee:
      - Zeige: Jeder Untermodul M' von M ist endlich erzeugt.
      - $K\cong P/I$, $M\cong P^r/U$ (siehe Definition 'Presentation einer R-Algebra')

- Damit sind Untermodule M' von M isomorph zu N/U, wobei N ein Untermodul von P^r ist.
- Wenn nun N und U endlich erzeugt sind, so ist es auch M'.
- Da N und U Untermodule von P^r sind, besitzen sie eine Gröbner-Basis, welche endlich ist.

2.4.2 Normalformen

- bisher: Kein eindeutiger Representant für eine Restklasse in P^r / M konnte gefunden werden.
- $m \in P^r, m \xrightarrow{G} m_G, m_G$ irreduzibel bzgl. $\xrightarrow{G} \Rightarrow m_G$ ist eindeutiger Representant für $\overline{m}$ und ist unabhängig von der gewählten Gröbner-Basis:
  - Beweis:
    - Sei H eine weitere Gröbner-Basis und $m \xrightarrow{H} m_H, m_H$ irreduzibel bzgl. $\xrightarrow{H}$.
    - Dann ist $m_G - m_H \in M$ ebenfalls irreduzibel und nach Bedingung C_2 $m_G - m_H = 0$.
    - also $m_G = m_H$
- Definition 'Normalform von m $\mathrm{NF}_{\sigma,M}(m)$': $\mathrm{NF}_{\sigma,M}(m) := m_G$
- $G := (g_1, \ldots, g_s)$, dann:
  - $\mathrm{NF}_{\sigma,M}(m) = \mathrm{NR}_{\sigma,G}(m)$
  - $\mathrm{NF}_{\sigma,M}(m_1 - m_2) = \mathrm{NF}_{\sigma,M}(m_1) - \mathrm{NF}_{\sigma,M}(m_2)$
  - $\mathrm{NF}_{\sigma,M}(\mathrm{NF}_{\sigma,M}(m)) = \mathrm{NF}_{\sigma,M}(m)$
- Untermodul Mitgliedsschafts Test: $M := \langle g_1, \ldots, g_s \rangle$, $N := \langle h_1, \ldots, h_t \rangle$, dann:
  - $\overline{m}_1 = \overline{m}_2 \Leftrightarrow \mathrm{NF}(m_1) = \mathrm{NF}(m_2)$
  - $\overline{m}_1 \in M \Leftrightarrow \overline{m}_1 = \overline{0} \Leftrightarrow \mathrm{NF}(m_1) = 0$
  - $N \subseteq M \Leftrightarrow \mathrm{NF}_M(h_i) = 0 \forall i$
  - $N = M \Leftrightarrow \mathrm{NF}_M(h_i) = 0 \forall i \wedge \mathrm{NF}_N(g_j) = 0 \forall j$
  - $N \subseteq M \wedge \mathrm{LT}\{M\} \subseteq \mathrm{LT}\{N\} \Rightarrow M = N$:
    - Beweis:
      - Wegen $N \subseteq M$ gilt $\mathrm{LT}\{M\} \supseteq \mathrm{LT}\{N\}$ automatisch und somit $\mathrm{LT}\{M\} = \mathrm{LT}\{N\}$.
      - Sei $m \in M$. Wegen $\mathrm{LT}\{M\} = \mathrm{LT}\{N\}$ ist $\mathrm{NF}_N(m) = \mathrm{NF}_M(m)$.
      - Da $m \in M$ ist $\mathrm{NF}_M(m) = 0$, also $\mathrm{NF}_N(m) = 0$, also $m \in N$, also $M \subseteq N$, also $M = N$.
- neue Version von Macaulay's Basis Theorem: G Gröbner-Basis von M, dann: $B := T^n \langle e_1, \ldots, e_r \rangle \setminus \underbrace{(\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))}_{\text{als Monomodul } \mathrm{LT}\{M\} \text{ aufgefasst}}$ ist eine Basis des ***K*-Vektorraums** P^r / M.

2.4.3 Reduced Gröbner-Basis

- Zu einer Gröbner-Basis können beliebige Elemente hinzugefügt werden und es bleibt eine Gröbner-Basis.
- Definition 'reduzierte σ-Gröbner-Basis':
  - $\mathrm{LC}(g_i) = 1 \forall i$
  - $(\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))$ ist ein minimales Erzeugendensystem von $\mathrm{LT}(M)$.
  - $\mathrm{Supp}(g_i - \mathrm{LT}(g_i)) \cap \mathrm{LT}\{M\} = \{\ \}$
- Existenz und Eindeutigkeit von reduzierten Gröbner-Basen: Es gibt immer eine

eindeutige reduzierte σ-Gröbner-Basis.:

- vorhandene Gröbner-Basis $(g_1,\ldots,g_s)$ in eine reduzierte verwandeln:
  1. g_i-s normieren
  2. $\{g_1,\ldots,g_t\}\in\{g_1,\ldots,g_s\}$ bestimmen, so dass $(\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t))$ ein minimales Erzeugendensystem von $\mathrm{LT}(M)$ ist.
  3. Nun: $g_i=\mathrm{LT}(g_i)+h_i$. Ersetze h_i durch $\mathrm{NF}(h_i)$, also $g_i:=\mathrm{LT}(g_i)+\mathrm{NF}(h_i)$.
- Definiton 'M definiert über k' (k Unterkörper von K): Es gibt Elemente aus $(k[x_1,\ldots,x_n])^r$, die M erzeugen.; 'Definitionskörper von M k': M ist definiert über k und es gibt keinen echten Unterkörper $k'\subset k$, über dem M definiert ist.
- K Körperweiterung von K', M' P'-Untermodul von $(P')^r$, M P-Untermodul von P^r von den Elementen aus M' erzeugt, dann:
  - Jede Gröbner-Basis von M' ist auch eine von M.
  - Die reduzierte Gröbner-Basis von M' ist auch die von M.
- Existenz und Eindeutigkeit des Definitionskörpers:
  - Es gibt einen eindeutigen Definitionskörper von M.
  - Der Definitionskörper von M ist der Körper erzeugt über dem Primkörper von K durch die Koeffizienten der Terme in den Supports der Vektoren der reduzierten Gröbner-Basis.

2.5 Buchberger's Algorithm

- Definition 'Menge der kritischen Paare B': $B:=\{(i,j)\mid 1\le i<j\le s,\gamma_i=\gamma_j\}$ 'S-Vektor/ S-Polynom von g_i und g_j': $S_{ij}:=\lambda(\sigma_{ij})=\frac{1}{c_i}t_{ij}g_i-\frac{1}{c_j}t_{ji}g_j$
- $S_{ij}\in M$:
  - Beweis: Folgt, weil G eine Gröbner-Basis ist und $S_{ij}\xrightarrow{G}0$, aus Bedingung C_1.
- $S_{ij}\xrightarrow{G}0$, dann: σ_{ij} hat eine Liftung in $\mathrm{Syz}(G)$:
  - Beweis: siehe 'University; Computational Commutative Algebra 1; Lecture Notes'
- Buchberger's Kriterium: G ist eine Gröbner-Basis von M. $\Leftrightarrow \mathrm{NR}_G(S_{ij})=0\,\forall(i,j)\in B$:
  - Beweis:
    - '$\Rightarrow$':
      - Gilt, weil $S_{ij}=\lambda(\sigma_{ij})=\frac{1}{c_i}t_{ij}g_i-\frac{1}{c_j}t_{ji}g_j\in M$ und G Gröbner-Basis ist.
    - '$\Leftarrow$':
      - $\mathrm{NR}_G(S_{ij})=0\Rightarrow S_{ij}\xrightarrow{G}0 \underbrace{\Rightarrow}_{\text{siehe Proposition von gerade}} \sigma_{ij}$ hat eine Liftung in $\mathrm{Syz}(G)\underbrace{\Rightarrow}_{D_3} G$ ist Gröbner-Basis
- Buchberger's Algirithmus: $\mathrm{LM}(g_i)=c_it_ie_{\gamma_i}$, dann:
  1. $s':=s$, $B:=\{(i,j)\mid 1\le i<j\le s,\gamma_i=\gamma_j\}$
  2. Falls $B=\{\}$, ist G eine Gröbner-Basis. Ansonsten wähle ein $(i,j)\in B$ und lösche es aus B.

3. Berechne S_{ij} und $\mathrm{NR}_G(S_{ij})$. Falls $\mathrm{NR}_G(S_{ij}) = 0$, gehe zu 2.
4. $s' := s' + 1$, $g_{s'} := \mathrm{NR}_G(S_{ij})$, $G := G \cup \{g_{s'}\}$, $B := B \cup \{(i,s') | 1 \le i < s', \gamma_i = \gamma_{s'}\}$ und gehe zu 2.

- Erste Optimierungen von Buchberger's Algorithmus:
  - Statt $\mathrm{NR}_G(S_{ij})$ zu berechnen reicht es ein Element m zu berechnen mit $S_{ij} \xrightarrow{G} m$ und $\mathrm{LT}(m) \notin (\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_{s'}))$.
  - $B' \subseteq B$, so dass $(\sigma_{ij} | (i,j) \in B')$ $\mathrm{Syz}(\mathrm{LM}(G))$ erzeugt, dann reicht es in Schritt 1 mit B' anzufangen.
  - 'normale Auswahl-Strategie': Wähle in Schritt 2 das (i,j), so dass $\mathrm{kgV}(t_i,t_j)$ bzgl. σ möglichst klein ist. Oder vereinfacht: Wähle in Schritt 2 das (i,j), so dass $\mathrm{kgV}(t_i,t_j)$ einen möglichst kleinen Grad hat.
- Definition 'triviale Syzygie von $f,g \in P$': $(-g,f)$
- Falls wir im 1-dimensionalen sind, also die g_i-s einfache Polynome sind, und $\mathrm{ggT}(t_i,t_j) = 1$, so hat σ_{ij} eine Liftung in $\mathrm{Syz}(G)$. M. a. W.: Wenn $\mathrm{ggT}(t_i,t_j) = 1$, so kann die trviale Syzygie von $(\mathrm{LM}(g_i),\mathrm{LM}(g_j))$ zu der trivialen Syzygie von (f,g) geliftet werden.
- Falls wir im 1-dimensionalen sind und die $\mathrm{LT}(g_i)$-s paarweise co-prim sind, dann ist G Gröbner-Basis.
- der erweiterte Buchberger Algorthmus: $\mathrm{LM}(g_i) = c_i t_i e_{\gamma_i}$, dann:
  1. $s' := s$, $A = I$ (Einheitsmatrix), $B := \{(i,j) | 1 \le i < j \le s, \gamma_i = \gamma_j\}$
  2. Falls $B = \{\}$, ist G eine Gröbner-Basis. Ansonsten wähle ein $(i,j) \in B$ und lösche es aus B.
  3. Berechne mit dem Divisionsalgorithmus eine Darstellung $S_{ij} = q_1 g_1 + \ldots + q_{s'} g_{s'} + p$. (Dann ist $p = \mathrm{NR}_G(S_{ij})$.) Falls $\mathrm{NR}_G(S_{ij}) = 0$, gehe zu 2.
  4. $s' := s' + 1$, $g_{s'} := \mathrm{NR}_G(S_{ij})$, $G := G \cup \{g_{s'}\}$, $B := B \cup \{(i,s') | 1 \le i < s', \gamma_i = \gamma_{s'}\}$, hänge den Spaltenvektor $\underbrace{\left(\frac{1}{c_i} t_{ij} \bar{a}_i - \frac{1}{c_j} t_{ji} \bar{a}_j - q_1 \bar{a}_1 - \ldots - q_{s'} \bar{a}_{s'}\right)}_{\text{Dies ist ein Spaltenvektor der Länge } s.}$ an A an und gehe zu 2.
- Der erweiterte Buchberger Algorithmus erzeugt eine Matrix A mit $G' = GA$.

2.6 Hilbert's Nullstellensatz

- Definition 'affine K-Algebra': endlich erzeugte K-Algebra
- Definition 'Menge der Nullstellen eines Ideals $I := (f_1,\ldots f_s) \subseteq P = K[x_1,\ldots,x_n]$ $Z(I)$': $Z(I) := \{(a_1,\ldots,a_n) \in \overline{K}^n | f(a_1,\ldots,a_n) = 0 \forall f \in I\}$
- $(a_1,\ldots,a_n) \in Z(I) \Leftrightarrow \begin{vmatrix} f_1(a_1,\ldots,a_n) = 0 \\ \vdots \\ f_s(a_1,\ldots,a_n) = 0 \end{vmatrix}$:
  - Beweis: klar

- Definition 'treuflach': $0 \to I \to P \to 0$ exakt $\Leftrightarrow 0 \to \bar{I} \to \bar{P} \to 0$ exakt
- Hilbert's Nullstellensatz (schwache Version): $Z(I) \neq \{\} \Leftrightarrow I \neq P$ bzw. $\Leftrightarrow 1 \notin I$
  - Hier wird oft nur $Z(I) \neq \{\} \Leftrightarrow \bar{I} \neq \bar{P}$ bewiesen.
  - $I \neq P \underbrace{\Leftrightarrow}_{\text{weil } \bar{K}[x_1,\ldots,x_n] \setminus K[x_1,\ldots,x_n] \text{ treuflach}} \bar{I} \neq \bar{P}$
- Hilbert's Nullstellensatz (körpertheoretische Version):
  - m maximales Ideal $\Rightarrow m \cap K[x_i] \neq (0)$
  - Die K-Algebra P/m ist ein algebraischer Erweiterungskörper von K von endlichem Grad.
- Definition 'Verschwindungsideal $I(S)$ $(S \subseteq \bar{K}^n)$: $\{f \in \bar{K}[x_1,\ldots,x_n] \mid f(a_1,\ldots,a_n) = 0 \forall (a_1,\ldots,a_n) \in S\}$
- Maximale Ideale von $\bar{P}$ haben die Form $(x_1 - a_1,\ldots,x_n - a_n)$, wobei $(a_1,\ldots,a_n) \in \bar{K}^n$.
- Das Verschwindungsideal ist ein Ideal.
  - Beweis: klar
- Verschiede Ideale können dieselbe Nullstellenmenge haben.
- Definition 'Radikal von I $\sqrt{I}$': $\{f \in R \mid f^i \in I \text{ für ein } i \geq 1\}$; 'Radikalideal': $\sqrt{I} = I$
- $Z(I) = Z(\sqrt{I})$:
  - Beweis: $\bar{a} \in Z(I) \Leftrightarrow f(\bar{a}) = 0 \forall f \in I \Leftrightarrow f^i(\bar{a}) = 0 \forall f \in I, i \geq 1 \Leftrightarrow \bar{a} \in Z(\sqrt{I})$
- Hilbert's Nullstellensatz (starke Version):
  - $I(Z(I)) = \sqrt{I}$
- Es gibt die Bijektion $\{\text{Radikalideale von } P\} \underset{I}{\overset{Z}{\rightleftarrows}} \{\text{Nullstellenmengen in } \bar{K}^n\}$.

3.1 Computation of Syzygies Modules

- Definition 'durch (σ, G) induzierte Ordnung auf $T^n\langle \varepsilon_1,\ldots,\varepsilon_s \rangle$ τ': $t\varepsilon_i \geq t'\varepsilon_j :\Leftrightarrow t\mathrm{LT}(g_i) >_\sigma t'\mathrm{LT}(g_j) \vee t\mathrm{LT}(g_i) =_\sigma t'\mathrm{LT}(g_j) \wedge i \leq j$
- τ ist eine Term-Ordnung.
- $\Sigma := \{\sigma_{ij} \mid (i,j) \in B\}$ ist eine τ-Gröbner-Basis von $\mathrm{Syz}(\mathrm{LM}(G))$.
- G σ-Gröbner-Basis von M, dann:
  - $\sigma_{ij} \in \mathrm{Syz}(G)$, d. h. $\lambda(\sigma_{ij}) = 0$, oder es gibt, weil G eine Gröbner-Basis ist, eine Darstellung $\lambda(\sigma_{ij}) = \sum_{k=1}^{s} f_{ijk} g_k$ mit

$$\deg_G(\sigma_{ij}) \underbrace{=}_{\text{nach Definition von } \deg_G} \max\left\{\mathrm{LT}\left(\frac{1}{c_i} t_{ij} g_i\right), \mathrm{LT}\left(-\frac{1}{c_j} t_{ji} g_j\right)\right\} \underbrace{\geq}_{\substack{\text{weil } \sigma_{ij} \in \mathrm{Syz}(\mathrm{LM}(G)), \\ \text{siehe auch Proposition 2.3.6.b}}} \mathrm{LT}(\lambda(\sigma_{ij}))$$

$$\underbrace{=}_{\text{nach } A_2} \max_k \{\mathrm{LT}(f_{ijk} g_k)\}$$

- Definition 's_{ij}': $s_{ij} := \begin{cases} \sigma_{ij}, \text{falls } \sigma_{ij} \in \text{Syz}(G) \\ \sigma_{ij} - \sum_{k=1}^{s} f_{ijk} g_k, \text{falls } \sigma_{ij} \notin \text{Syz}(G) \end{cases}$
- $\{s_{ij} | (i,j) \in B\}$ ist eine τ-Gröbner-Basis von $\text{Syz}(G)$
- $\{\sigma_{ij} | (i,j) \in B' \subseteq B\}$ erzeugt $\text{Syz}(\text{LM}(G)) \Rightarrow \{s_{ij} | (i,j) \in B'\}$ erzeugt $\text{Syz}(G)$

- Berechnung des Syzygien-Moduls von Gröbner-Basen:
  1. Initialisiere M als $s \times 0$-Matrix (s Zeilen, 0 Spalten) und $B := \{(i,j) | 1 \le i < j \le s, \gamma_i = \gamma_j\}$.
  2. Falls $B = \{\}$, bilden die Spalten von M eine τ-Gröbner-Basis von $\text{Syz}(G)$. Ansonsten wähle ein $(i,j) \in B$ und lösche es aus B.
  3. Berechne S_{ij}. Falls $S_{ij} \neq 0$, berechne mit dem Divisionsalgorithmus eine Darstellung $S_{ij} = f_{ij1} g_1 + \ldots + f_{ijs} g_s$.
  4. Falls $S_{ij} = 0$, füge σ_{ij} als Spaltenvektor M hinzu; falls $S_{ij} \neq 0$ füge $\sigma_{ij} - \sum_{k=1}^{s} f_{ijk} \varepsilon_k$ als Spaltenvektor M hinzu; gehe zu 2.
- Berechnung von Syzygien-Moduln (H Erzeugendensystem für Modul M; Matrix M (hat nichts mit dem Modul M zu tun, einfach eine Bezeichnung für 2 verschieden Dinge) Erzeugendensystem für $\text{Syz}(G)$):
  - Es gilt also: $GM = \begin{pmatrix} \underbrace{\vec{0}}_{\in P^r} & \cdots & \vec{0} \end{pmatrix}$.
  1. Berechne mit dem erweiterten Buchberger Algorithmus aus H eine Gröbner-Basis G mit $G = HA$.
  2. Berechne mit dem Divisionsalgorithmus $h_j = b_{1j} g_1 + \ldots + b_{sj} g_s$ und daraus $H = GB$
  - Es gilt $\begin{pmatrix} \vec{0} & \cdots & \vec{0} \end{pmatrix} = GM = HAM$, also $AM \subseteq \text{Syz}(H)$, und es gilt $H = GB = HAB \Leftrightarrow H - HAB = \begin{pmatrix} \vec{0} & \cdots & \vec{0} \end{pmatrix} \Leftrightarrow H(I - AB) = \begin{pmatrix} \vec{0} & \cdots & \vec{0} \end{pmatrix}$, also $(I - AB) \subseteq \text{Syz}(H)$.
  - Insgesamt gilt: $N := (AM \mid I - AB) = \text{Syz}(H)$.
- Explizite Mitgliedschaft:
  - $m \in M$ bzgl. G gegeben ($m = \sum_{i=1}^{s} f_i g_i$); Ziel: Darstellung von m bzgl. H.
  - $m = G\vec{f} = (HA)\vec{f} = H\underbrace{(A\vec{f})}_{=:\vec{q}}$, also ist $m = \sum_{i=1}^{t} \vec{q}_i h_i$ die gesuchte Darstellung.
- Wenn der erweiterte Buchberger Algorithmus verwendet wurde, ist $A = \begin{pmatrix} \underbrace{I_t}_{t \times t} \mid \underbrace{C}_{t \times (s-t)} \end{pmatrix}$.

  Decompose $M = \begin{pmatrix} \overbrace{M'}^{t \text{ Zeilen}} \\ \underbrace{M''}_{s-t \text{ Zeilen}} \end{pmatrix}$. Dann: $\text{Syz}(H)$ wird erzeugt von $M' + C \cdot M''$.:
  - Beweis:
    - G wurde aus H gebildet, indem Vektoren angehängt wurden. Daher $H = GB \Rightarrow B = \begin{pmatrix} I_t \\ 0 \end{pmatrix}$.

- daher: $\mathrm{Syz}(H) = N = \left(AM \mid I - \underbrace{A}_{=(I_t \mid C)} \underbrace{B}_{=\binom{I_t}{0}} \right) = (AM \mid I - I) = (AM \mid 0) = \left((I_t \mid C) \begin{pmatrix} M' \\ M'' \end{pmatrix} \mid 0 \right)$
- also $\mathrm{Syz}(H) = M' + C \cdot M''$

- Iteratives finden eines irredundanten Erzeugendensystems von M (erzeugt durch H):
  - $h_i \in \langle h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_t \rangle \Leftrightarrow$ Das durch die i-te Zeile von N erzeugte Ideal ist das Einheitsideal von P, das heißt es enthält die 1.:
    - Beweis:
      - Angenommen, es gibt in der i-ten Zeile von N bereits eine 1 in Spalte j. Dann ist $\sum_{k=1}^{t} n_{kj} h_k = 0 \Leftrightarrow \sum_{k=1}^{i-1} n_{kj} h_k + \underbrace{n_{ij}}_{=1} h_i + \sum_{k=i+1}^{t} n_{kj} h_k = 0 \Leftrightarrow h_i = -\left(\sum_{k=1}^{i-1} n_{kj} h_k + \sum_{k=i+1}^{t} n_{kj} h_k \right)$.
      - Also $h_i \in \langle h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_t \rangle$.
      - Außerdem ist offensichtlich die 1 in dem von der i-ten Spalte erzeugten Ideal.
      - Es ist leicht einzusehen, dass es bereits reicht, wenn die 1 in dem von der i-ten Spalte erzeugten Ideal liegt.

3.2 Elementary Operations on Modules

- $M := \langle g_1, \ldots, g_s \rangle$, $N := \langle h_1, \ldots, h_t \rangle$, $I := \langle f_1, \ldots, f_u \rangle$ (Ideal), dann:
  - $M + N = \langle g_1, \ldots, g_s, h_1, \ldots, h_t \rangle$
  - $I \cdot M = \langle f_1 g_1, \ldots, f_1 g_s, f_2 g_1, \ldots, f_2 g_s, \ldots, f_u g_1, \ldots, f_u g_s \rangle$
  - $I^d = \left\langle f_{i_1} \cdot \ldots \cdot f_{i_d} \middle| i_j \in \{1, \ldots, u\} \right\rangle$

3.2.1 Intersections

- $\langle v_1, \ldots, v_u \rangle \subseteq P^{s+t}$ Erzeugendensystem von $\mathrm{Syz}(g_1, \ldots, g_s h_1, \ldots, h_t)$ mit $v_j = \begin{pmatrix} f_{1;j} \\ \vdots \\ f_{s+t;j} \end{pmatrix}$,

  $\lambda(\varepsilon_i) = g_i$, dann: $\lambda^{-1}(N) = \left\langle \left(f_{1j}, \ldots, f_{sj} \right) \middle| 1 \le j \le u \right\rangle$.
  - Beweis: $\underbrace{\sum_{i=1}^{s} f_{ij} g_i}_{\in M} + \underbrace{\sum_{i=1}^{t} f_{s+i;j} h_i}_{\in N} = 0 \Leftrightarrow \sum_{i=1}^{s} f_{ij} g_i = \underbrace{-\sum_{i=1}^{t} f_{s+i;j} h_i}_{=:n} \Leftrightarrow \begin{pmatrix} f_{1j} \\ \vdots \\ f_{sj} \end{pmatrix} = \lambda^{-1}(n)$
- Schnitt von 2 Untermoduln:
  - $M \cap N = \lambda\left(\lambda^{-1}(N)\right) = \left\langle \sum_{i=1}^{s} f_{ij} g_i \middle| 1 \le j \le u \right\rangle$
    - Beweis: folgt aus $\lambda^{-1}(N) = \left\langle \left(f_{1j}, \ldots, f_{sj} \right) \middle| 1 \le j \le u \right\rangle$
  - jetzt: $M := \begin{pmatrix} I_r & G & 0 \\ I_r & 0 & H \end{pmatrix}$, $\mathrm{Syz}(M) = \langle v_1, \ldots, v_u \rangle \subseteq P^{r+s+t}$ mit $v_j = \begin{pmatrix} f_{1;j} \\ \vdots \\ f_{r+s+t;j} \end{pmatrix}$, dann:

$$M \cap N = \left\langle \begin{pmatrix} f_{1j} \\ \vdots \\ f_{rj} \end{pmatrix} \middle| 1 \le j \le u \right\rangle$$

- Beweis:
  - $$I_r \begin{pmatrix} f_{1j} \\ \vdots \\ f_{rj} \end{pmatrix} + G \begin{pmatrix} f_{r+1;j} \\ \vdots \\ f_{r+s;j} \end{pmatrix} + 0 \begin{pmatrix} f_{r+s+1;j} \\ \vdots \\ f_{r+s-t;j} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in P^r$$
  - $$I_r \begin{pmatrix} f_{1j} \\ \vdots \\ f_{rj} \end{pmatrix} + 0 \begin{pmatrix} f_{r+1;j} \\ \vdots \\ f_{r+s;j} \end{pmatrix} + H \begin{pmatrix} f_{r+s+1;j} \\ \vdots \\ f_{r+s-t;j} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in P^r$$
  - also: $\begin{pmatrix} f_{1j} \\ \vdots \\ f_{rj} \end{pmatrix} = -G \begin{pmatrix} f_{r+1;j} \\ \vdots \\ f_{r+s;j} \end{pmatrix} \in M$
  - also: $\begin{pmatrix} f_{1j} \\ \vdots \\ f_{rj} \end{pmatrix} = -H \begin{pmatrix} f_{r+s+1;j} \\ \vdots \\ f_{r+s-t;j} \end{pmatrix} \in N$
  - also: $\begin{pmatrix} f_{1j} \\ \vdots \\ f_{rj} \end{pmatrix} \in M \cap N$

- Definition ‘Presentation von M via Erzeuger und Relationen’ ($\psi\left(\underbrace{\vec{e}_j}_{\in R^u}\right) := v_j$, $\varphi\left(\underbrace{\vec{e}_i}_{\in R^s}\right) := m_i$):

  $R^u \xrightarrow{\psi} R^s \xrightarrow{\varphi} M \to 0$
- $M \cong R^s / \langle v_1, \ldots, v_u \rangle$
- $w_j := \begin{pmatrix} f_{1j} \\ \vdots \\ f_{sj} \end{pmatrix}$, wobei $v_j := \begin{pmatrix} f_{1;j} \\ \vdots \\ f_{s+t;j} \end{pmatrix}$ der j-te Erzeuger von $\mathrm{Syz}(\langle g_1, \ldots, g_s, h_1, \ldots, h_t \rangle)$, $\overline{\lambda} : P^s \to M/(M \cap N)$ die von λ induzierte Abbildung, $\psi : \begin{matrix} P^u \to P^s \\ \vec{e}_j \mapsto w_j \end{matrix}$, dann: $P^u \xrightarrow{\psi} P^s \xrightarrow{\overline{\lambda}} M/(M \cap N) \to 0$ ist eine Presentation von $M/(M \cap N)$.
- Berechnung von mehrfachen Schnitten:
  - $(M_1 \cap \ldots \cap M_l) = (M_1 \cap \ldots \cap M_{l-1}) \cap M_l$
  - $M := \begin{pmatrix} I_r & M_1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ I_r & 0 & \cdots & 0 & M_l \end{pmatrix}$
- Berechnung von ggT und kgV:
  - Berechne die reduzierte Gröbner-Basis des Schnittmengen-Ideals $(f_1) \cap \ldots \cap (f_m)$,

dann: Diese Gröbner-Basis besteht nur aus dem einen Element $\mathrm{kgV}(f_1,\ldots,f_m)$.

- $\mathrm{ggT}(f_1,f_2)=\frac{f_1 f_2}{\mathrm{kgV}(f_1,f_2)}$, $\mathrm{ggT}(f_1,\ldots,f_m)=\mathrm{ggT}(\mathrm{ggT}(f_1,\ldots,f_{m-1}),f_m)$

3.2.2 Colon Ideals and Annihilators

- Defintion 'Colon Ideal': $N:_R M:=\{r\in R \mid r\cdot M\subseteq N\}$; 'Annihilator von M': $\mathrm{Ann}_R(M):=\{r\in R \mid r\cdot M=0\}$
- $N:_R M=\mathrm{Ann}_R(M/M\cap N)$:
  - Beweis:
    $\mathrm{Ann}_R(M/M\cap N)=\{r\in R \mid r\cdot M\subseteq M\cap N\} \underbrace{=}_{\text{weil automatisch } r\cdot M\subseteq M} \{r\in R \mid r\cdot M\subseteq N\}=N:_R M$
- Remark 3.2.12
- $N:=\langle h_1,\ldots,h_t\rangle$, $\langle v_1,\ldots,v_u\rangle=\mathrm{Syz}(g,h_1,\ldots,h_t)$, $v_j=\begin{pmatrix} r_j \\ s_{1j} \\ \vdots \\ s_{tj}\end{pmatrix}$, dann: $N:_R\langle g\rangle=(r_1,\ldots,r_u)$
  - Beweis: $N:_R\langle g\rangle=\{r\in R \mid r\cdot\langle g\rangle\subseteq N\} \hat{\Leftrightarrow} r\underbrace{g'}_{\in\langle g\rangle}=\underbrace{s_1h_1+\ldots+s_th_t}_{\in N} \Leftrightarrow \begin{pmatrix} r \\ s_1 \\ \vdots \\ s_t\end{pmatrix}\in\mathrm{Syz}(g,h_1,\ldots,h_t)$
- Berechnung von Colon Idealen: $M:=\langle g_1,\ldots,g_s\rangle$, $N:=\langle h_1,\ldots,h_t\rangle$, dann:
  - $N:_P M=\mathrm{Ann}_P(M/M\cap N)=\bigcap_{i=1}^{s}(N:_P\langle g_i\rangle)$
    - Beweisidee: Zeige $\{r\in R \mid r\cdot M\subseteq N\}=\bigcap_{i=1}^{s}\{r\in R \mid r\cdot\langle g_i\rangle\subseteq N\}$ durch '$\subseteq$' und '$\supseteq$'.
  - $L:=\underbrace{\begin{pmatrix} g_1 & H & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ g_s & 0 & \cdots & 0 & H\end{pmatrix}}_{(sr)\times(1+ts)}$, $\langle v_1,\ldots,v_u\rangle=\mathrm{Syz}(L)$, $v_j=\begin{pmatrix} r_j \\ s_{1;j} \\ \vdots \\ s_{ts;j}\end{pmatrix}$, dann: $N:_R M=(r_1,\ldots,r_u)$
    - Beweisidee: Benutze $N:_R\langle g\rangle=(r_1,\ldots,r_u)$.

3.2.3 Colon Modules

- Definition 'Colon Modul': $N:_M I:=\{m\in M \mid I\cdot m\subseteq N\}$
- Proposition 3.2.18
- $M:=\langle g_1,\ldots,g_s\rangle$, $N:=\langle h_1,\ldots,h_t\rangle$, $fM\cap N=\langle v_1,\ldots,v_u\rangle$ (somit $v_i=fw_i$ für irgendein $w_i\in M$, denn $v_i\in fM$, denn $v_i\in fM\cap N$), dann:
  - $N:_M(f)=\langle w_1,\ldots,w_u\rangle$
    - Beweis:
      - '$\subseteq$':

$$m \in N :_M (f) \Rightarrow fm \in \underbrace{fM}_{\text{trivialer Weise}} \cap N \Rightarrow m = \sum_{i=1}^{u} a_i v_i = \sum_{i=1}^{u} a_i f w_i$$

$$= f \underbrace{\sum_{i=1}^{u} a_i w_i}_{\in \langle w_1,\ldots,w_u \rangle} \in \langle w_1,\ldots,w_u \rangle$$

- '$\supseteq$': $fw_i = v_i \in fM \cap N \subseteq N \Rightarrow w_i \in N :_M (f)$

- $\mathrm{Syz}(fg_1,\ldots,fg_s,h_1,\ldots,h_t) = \langle \tilde{v}_1,\ldots,\tilde{v}_l \rangle$, $\tilde{v}_j = \begin{pmatrix} f_{1;j} \\ \vdots \\ f_{s+t;j} \end{pmatrix}$, dann: $N :_M (f) = \left\langle \sum_{i=1}^{s} f_{ij} g_i \right\rangle$

  - Beweis:
    $N :_M (f) = \{ m \in M \mid fm \subseteq N \} \Leftrightarrow f(\underbrace{f_1 g_i + \ldots + f_s g_s}_{=m}) = f_{s+1} h_1 + \ldots + f_{s+t} h_t$

    $\Leftrightarrow \begin{pmatrix} f_1 \\ \vdots \\ f_{s+t} \end{pmatrix} \in \mathrm{Syz}(fg_1,\ldots,fg_s,h_1,\ldots,h_t)$

- Berechnung von Colon Moduln: $M := \langle g_1,\ldots,g_s \rangle$, $N := \langle h_1,\ldots,h_t \rangle$, $I := \langle f_1,\ldots,f_l \rangle$, dann:

  - $N :_M I = \bigcap_{i=1}^{l} (N :_M \langle f_i \rangle)$

    - Beweisidee: Zeige $\{ m \in M \mid I \cdot m \subseteq N \} = \bigcap_{i=1}^{l} \{ m \in M \mid \langle f_i \rangle \cdot m \subseteq N \}$ durch '$\subseteq$' und '$\supseteq$'.

  - $L := \underbrace{\begin{pmatrix} f_1 G & H & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ f_l G & 0 & \cdots & 0 & H \end{pmatrix}}_{(lr)\times(s+tl)}$, $\langle v_1,\ldots,v_u \rangle = \mathrm{Syz}(L)$, $v_j = \begin{pmatrix} f_{1;j} \\ \vdots \\ f_{s;j} \\ f_{s+1;j} \\ \vdots \\ f_{s+tl;j} \end{pmatrix}$, dann: $N :_M I = \left\langle \sum_{i=1}^{s} f_{ij} g_i \right\rangle$

    - Beweisidee: Benutze $N :_M (f) = \left\langle \sum_{i=1}^{s} f_{ij} g_i \right\rangle$.

- Definition 'Nicht-Nullteiler für U $f \in R$': $f \cdot m = 0 \Rightarrow m = \bar{0}$; 'reguläre Sequenz für U $(f_1,\ldots,f_l)$': $(f_1,\ldots,f_l)U \neq U \wedge f_i$ ist Nicht - Nullteiler für $U/(f_1,\ldots,f_{i-1})U \forall 1 \leq i \leq l$
- Corollary 3.2.24

3.3 Homomorphisms of Moduls

- left out

3.4 Elimination

- Definition 'Eliminations-Ideal von I bzgl. $\{x_{j+1},\ldots,x_n\}$': $I \cap K[x_1,\ldots,x_j]$

- Definition '$\hat{P}$' ($L \subseteq \{x_1,\ldots,x_n\}$): $\hat{P} := K[x_i \mid x_i \notin L]$
- Definition 'Eliminations-Ordnung σ': σ ist Modul-Termordnung und $\mathrm{LT}(m) \in \hat{P}^r \Rightarrow m \in \hat{P}^r$.; 'Eliminations-Modul von M bzgl. L $\hat{M}$': $\hat{M} := M \cap \hat{P}^r$
- Definition '$\hat{T}\langle e_1,\ldots,e_r\rangle$': $\hat{T}\langle e_1,\ldots,e_r\rangle := T\langle e_1,\ldots,e_r\rangle \cap \hat{P}^r$; '$\hat{\sigma}$': $\hat{\sigma} := \sigma_{|\hat{T}\langle e_1,\ldots,e_r\rangle}$
- σ Modul-Ordnung $\Rightarrow$ $\hat{\sigma}$ Modul-Ordnung
- σ Modul-Term-Ordnung $\Rightarrow$ $\hat{\sigma}$ Modul-Term-Ordnung
- Berechnung von Eliminations-Moduln:
  - $\mathrm{LT}_{\hat{\sigma}}\left(M \cap \hat{P}^r\right) = \mathrm{LT}_{\sigma}(M) \cap \hat{P}^r$
    - Beweis:
      - '$\subseteq$': $te_i \in \mathrm{LT}_{\hat{\sigma}}\left(M \cap \hat{P}^r\right) \Rightarrow te_i \in \underbrace{\mathrm{LT}_{\sigma}(M)}_{\supseteq \mathrm{LT}_{\hat{\sigma}}\left(M \cap \hat{P}^r\right)} \wedge te_i \in \hat{P}^r \Rightarrow \mathrm{LT}_{\sigma}(M) \cap \hat{P}$
      - '$\supseteq$':
        $te_i \in \mathrm{LT}_{\sigma}(M) \cap \hat{P} \Rightarrow te_i \in \mathrm{LT}_{\sigma}(M) \wedge te_i \in \hat{P}^r \underbrace{\Rightarrow}_{\text{da } \sigma \text{ Eliminationsordnung}} \exists g_i \in \hat{P}^r : te_i = \mathrm{LT}_{\sigma^r}(g_i)$
        $\Rightarrow \mathrm{LT}_{\hat{\sigma}}\left(M \cap \hat{P}^r\right)$
  - G σ-Gröbner-Basis von M $\Rightarrow$ $\hat{G} := G \cap \hat{P}^r$ $\hat{\sigma}$-Gröbner-Basis für $\hat{M} = M \cap \hat{P}^r$
    - Beweis: Folgt aus gerade Gezeigtem.
  - G reduzierte σ-Gröbner-Basis von M $\Rightarrow$ $\hat{G} := G \cap \hat{P}^r$ reduzierte $\hat{\sigma}$-Gröbner-Basis für $\hat{M} = M \cap \hat{P}^r$
    - Beweis: Folgt aus gerade Gezeigtem.
- $M := \langle g_1,\ldots,g_s\rangle$, $N := \langle h_1,\ldots,h_t\rangle$, $U := \langle yg_1,\ldots,yg_s,(1-y)h_1,\ldots(1-y)h_t\rangle \subseteq P[y]$, dann: $M \cap N = U \cap P^r$
  - Beweis:
    $$v \in M \cap N \Leftrightarrow v = \sum_{i=1}^{s} p_i g_i = \sum_{i=1}^{t} q_i h_i \Leftrightarrow v = yv + (1-y)v = y\sum_{i=1}^{s} p_i g_i + (1-y)\sum_{i=1}^{t} q_i h_i$$
    $$= \sum_{i=1}^{s} \underbrace{(p_i y)}_{\in P[y]} g_i + \sum_{i=1}^{t} \underbrace{(q_i(1-y))}_{\in P[y]} h_i \in U \cap P^r$$
- $1 \le i \le l$, $M_i := \langle g_{i1},\ldots,g_{is_i}\rangle$, $U := \{y_i g_{ij}\} \cup \{(1-y_1-\ldots-y_l)e_i\} \subseteq P[y_1,\ldots,y_l]$, dann $\bigcap_{i=1}^{l} M_i = U \cap P^r$
  - Beweis: wie eben
- $M := \langle g_1,\ldots,g_s\rangle$, $N := \langle h_1,\ldots,h_t\rangle$, dann:
  - $f \in P$, $U := \{fyg_1,\ldots,fyg_s,(1-y)h_1,\ldots,(1-y)h_t\}$,
    $\underbrace{v_i}_{\text{einer der Erzeuger von } U\cap P^r}$ $\underbrace{=}_{\text{weil } U\cap P^r = fM\cap N \text{ (vgl. oben: } U \text{ ähnlich definiert, d. h. ohne } f\text{-s, dann: } U\cap P^r = M\cap N)}$ fw_i dann: $N :_M (f) = \langle w_1,\ldots,w_u\rangle$
  - $I := (f_1,\ldots,f_l)$, $f(y) = f_1 + f_2 y + f_l y^{l-1} \in P[y]$, dann $N :_M I = \left(NP[y] :_{MP[y]} (f(y))\right) \cap P^r$

3.5 Localization and Saturation

3.5.1 Localization

- Definition 'multiplikativ abgeschlossene Menge $S \subseteq R$':
  - $1_R \in S$
  - $a,b \in S \Rightarrow ab \in S$
- Definition '$(m,s) \sim (m',s')$' (M R-Modul, S multiplikativ abgeschlossene Menge von R): $(m,s) \sim (m',s') := \exists s'' : s''(s'm - sm') = 0$; '$M_S$': Menge aller Äquivalenzklassen; '$\frac{m}{s}$': die Äquivalenzklasse von (m,s)
- Mit $\frac{m}{s} + \frac{m'}{s'} := \frac{s'm + sm'}{ss'}$ und $r \cdot \frac{m}{s} := \frac{rm}{s}$ wird M_S zu einem R-Modul.
- Einbettung: $\begin{matrix} M \to M_S \\ m \mapsto \frac{m}{1} \end{matrix}$
- Mit $\frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}$ wird R_S zu einem Ring.
- Mit $\frac{r}{s} \cdot \frac{m}{s'} := \frac{rm}{ss'}$ wird M_S zu einem R_S-Modul.
- Die Einbettung $\begin{matrix} R \to R_S \\ r \mapsto \frac{r}{1} \end{matrix}$ ist ein R-Algebren-Homomorphismus.
- Definition 'Lokalisation von M in S/ Brüche-Modul von M bzgl. S': der R_S-Modul M_S
- Definition 'M_f': $M_f := M_S$ mit $S := \{f^i\}$
- $0 \in S \Rightarrow M_S = 0$
  - Beweis:
    - $\frac{m}{s} \sim \frac{0}{1} \forall \frac{m}{s} \in M_S$, denn $\frac{m}{s} \sim \frac{0}{1} \Leftrightarrow \exists s'' : s''(1 \cdot m - s \cdot 0) = 0$
    - Wähle $s'' := 0 \in S$
- $M_S = 0 \Leftrightarrow \mathrm{Ann}_R(M) \cap S \neq \{\}$:
  - Beweis:
    - $\frac{m}{s} \sim \frac{0}{1} \forall \frac{m}{s} \in M_S$, denn $\frac{m}{s} \sim \frac{0}{1} \Leftrightarrow \exists s'' : s''(1 \cdot m - s \cdot 0) = 0$
    - Wähle $s'' \in \mathrm{Ann}_R(M) \cap S$
- erweiterte Division: $f \in R[x_1,\ldots,x_n]$, $g(y) \in R[x_1,\ldots,x_n][y] \Rightarrow \exists q(y) \in R[x_1,\ldots,x_n][y], r \in R[x_1,\ldots,x_n] : f^{\deg g} g(y) = q(y) \cdot (fy - 1) + r$
- $R_f \cong R[y]/(fy - 1)$

3.5.2 Saturation

- Definition 'Sättigung von N durch I in M': $N :_M I^\infty := \left\{ m \in M \middle| \exists i \in \mathrm{N}_0 : I^i m \subseteq N \right\}$
- Proposition 3.5.8
- $\exists k : N :_M I^\infty = N :_M I^k = N :_M I^{k+1} = \ldots$
  - Beweisidee: Gilt, weil $N :_M I \subseteq N :_M I^2 \subseteq \ldots \subseteq M$ und M noetherian.
- Sättigung und Lokalisation ($I = \langle f \rangle$): $N :_M I^\infty = N_f \cap M$
- $(N :_M I^\infty) \cap (N :_M J^\infty) = N :_M (I + J)^\infty$

- Beweis:
  - '$\subseteq$':
    $v \in (N :_M I^\infty) \cap (N :_M J^\infty) \Leftrightarrow \exists i, j : I^i v \subseteq N \wedge J^j v \subseteq N$
    $\Leftrightarrow \exists i, j : f^i v \in N \wedge g^j v \in N \forall f \in I, g \in J \Rightarrow (f+g)^{i+j} v \in N \forall f \in I, g \in J$,
    $\Rightarrow v \in N :_M (I+J)^\infty$
    wobei die letzte Folgerung gilt, weil
    $(f+g)^{i+j} v \underbrace{=}_{\text{bis auf Konstanten bei den Summanden}} \underbrace{f^{i+j} g^0 v + f^{i+j-1} g^1 v + \ldots}_{\in N \text{ wegen } f^k \underbrace{(f^i v)}_{\in N} \in N \text{ für } 1 \le k \le j} + \underbrace{f^i g^j v}_{\text{offensichtlich} \in N} + \underbrace{\ldots + f^1 g^{i+j-1} v + f^0 g^{i+j} v}_{\in N \text{ wegen } g^k \underbrace{(g^i v)}_{\in N} \in N \text{ für } 1 \le k \le j}$
  - '$\supseteq$':
    $v \in N :_M (I+J)^\infty \Leftrightarrow \exists k : (I+J)^k v \subseteq N \Leftrightarrow \exists k : (f+g)^k v \in N \forall f \in I, g \in J$
    $\Rightarrow \left(f + \underbrace{0}_{\in J}\right)^k v \in N \wedge \left(\underbrace{0}_{\in I} + g\right)^k v \in N \forall f \in I, g \in J \Rightarrow f^k v \in N \wedge g^k v \in N \forall f \in I, g \in J$
    $\Rightarrow v \in (N :_M I^\infty) \cap (N :_M J^\infty)$
- Berechnung von Sättigungen:
  - $N :_M (f)^\infty = (NP[y] + (fy-1) \cdot P[y]^r) \cap M$
  - $I = \langle f_1, \ldots, f_s \rangle$, dann: $N :_M I^\infty = \bigcap_{i=1}^{s} N :_M (f_i)^\infty$
  - $I = \langle f_1, \ldots, f_s \rangle$, $f(y) := f_1 + f_2 y + \ldots + f_s y^{s-1}$, dann: $N :_M (f)^\infty = (NP[y] :_{P[y]^r} (f(y))^\infty) \cap M$

  $f \in \sqrt{I}$
  $\Leftrightarrow IP_f = P_f$
- $\Leftrightarrow 1 \in I :_P (f)^\infty$
  $\Leftrightarrow 1 \in IP[y] + (fy+1)$
  $\Leftrightarrow$ Jede Gröbner - Basis des Ideals $IP[y] + (fy+1)$ enthält ein Element aus $K \setminus \{0\}$.
  $\Leftrightarrow$ Die reduzierte Gröbner - Basis des Ideals $IP[y] + (fy+1)$ ist (1).

3.6 Homomorphisms of Algebras

- left out

Remarks

Der erste Teil dieser Übersicht bezieht sich auf die Grundlagen der ‘Algebra 1’-Vorlesung von Prof. Martin Kreuzer im Wintersemester 2003/2004. Zu dieser Vorlesung gibt es eine Fotoreihe der Tafeln (Dateien: University; Algebra 1; WS 2003; *).
Der zweite Teil dieser Übersicht bezieht sich auf die ‘Computanional Commutative Algebra 1 (Algebra 2)’-Vorlesung von Prof. Martin Kreuzer im Sommersemester 2004 und das Buch ‘Computanional Commutative Algebra 1’ von Martin Kreuzer und Lorenzo Robbiano (Version vom 2000-07-03). Zu dieser Vorlesung gibt es eine Fotoreihe der Tafeln (Dateien: University; Computational Commutative Algebra 1 (Algebra 2); SS 2004; *). Außerdem gibt es eine weitere Datei ‘University; Computational Commutative Algebra 1; Lecture Notes’, welche viele Ergänzungen/ Erklärungen (hauptsächlich zu Beweisen) enthält – sowohl zur Vorlesung, als auch zum Buch.

http://www.TL-Software.de.tf
thleopold@hotmail.com

Thomas Leopold,
2004-10-13