Humboldt-Universität zu Berlin
Institut für Mathematik
Wintersemester 2009/2010

Algebra I

Prof. Farkas

Bodo Graumann

19. Mai 2014

Inhaltsverzeichnis

Der Code wurde mit `gvim` sowie `vim-latex` erstellt und mit `xelatex` kompiliert – all das auf `Gentoo Linux`. Meinen Dank an die Freie Software Community und die TEX-Kollegen auf TEX.SX für ihre Hinweise und Unterstützung.
Bitte schreibt mir eure Kommentare und Verbesserungsvorschläge zu diesem Dokument! Ihr könnt mir entweder direkt mailen oder das Kontaktformular auf meiner Internetseite benutzen.

1 Gruppentheorie

1.1 Wiederholung

1 **Definition: „Gruppe“**

Eine Gruppe ist ein Paar $(G, \cdot)$ mit den Eigenschaften

1. $\forall x, y, z \in G: x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $\exists e \in G \forall x \in G: x \cdot e = e \cdot x = x$, e heißt das neutrale Element der Gruppe
3. $\forall x \in G \exists x^{-1} \in G: x \cdot x^{-1} = x^{-1} \cdot x = e$

G heißt abelsch falls $\forall x, y \in G: x \cdot y = y \cdot x$.

2 **Definition: „Gruppenhomomorphismus“**

Ein Gruppenhomomorphismus ist eine Abbildung zwischen zwei Gruppen $\varphi: G \to G'$ für die gilt:

$$\forall x, y \in G: \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

Beispiele

- die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ der Restklassen modulo n
- die symmetrische Gruppe S_n der Permutationen von n Elementen
- die Automorphismengruppe $GL(V)$ für einen Vektorraum V und die Gruppe der zugehörigen Matrizen $GL_n(k)$
- die Gruppe der Orthogonalen Matrizen $\mathbb{O}_n(k)$

3 **Definition: „Untergruppe“**

Ist G eine Gruppe, dann heißt ein $H \subseteq G, H \neq \varnothing$ Untergruppe von G genau dann, wenn

$$\forall x, y \in H: xy^{-1} \in H$$

Man schreibt $H \leq G$.

4 **Bemerkung: Unterraumkriterien**

$H \leq G$ ist äquivalent zu den drei Bedingungen:

$$\forall x, y \in H: xy \in H$$
$$e \in H$$
$$\forall x \in H: x^{-1} \in H$$

5 **Definition: „Bild, Kern“**

Ist $\varphi: G \to G'$ ein Gruppenhomomorphismus, dann ist der Kern von φ

$$\ker \varphi := \varphi^{-1}(e_{G'})$$

und das Bild

$$\operatorname{im} \varphi := \varphi(G)$$

6 **Lemma: Eigenschaften von Kern und Bild**

$$\ker \varphi \leq G$$
$$\operatorname{im} \varphi \leq G'$$

φ ist genau dann injektiv, wenn $\ker \varphi = \{e\}$ ist.

1.2 Direkte Produkte und Summen

7 **Definition: „direktes Produkt“**

Sei I eine beliebige Indexmenge und $(G_i)_{i\in I}$ eine Familie von Gruppen, dann ist das direkte Produkt

$$G = \prod_{i\in I} G_i := \left\{ g = (g_i)_{i\in I} \;\middle|\; \forall_{i\in I}: g_i \in G_i \right\}$$

G ist wiederum eine Gruppe wobei die Gruppenoperation elementweise angewendet wird:

$$\forall g, h \in G: g \cdot h = \left(g_i\right)_{i\in I} \cdot \left(h_i\right)_{i\in I} := \left(g_i \cdot h_i\right)_{i\in I}$$

Also sind auch das neutrale und die inversen Elemente elementweise zu erhalten.

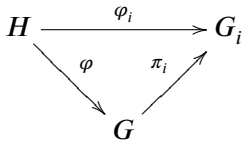
8 **Definition: „Projektion“**

Eine Projektion von G auf $J \subseteq I$ ist die Einschränkung der $g_i \in G$ auf die Indizes aus J und wird als π_J bzw. für $J = \{j\}$ als π_j bezeichnet.

9 **Satz: Universelle Eigenschaft des direkten Produktes**

Ist H eine Gruppe und $\left\{\varphi_i: H \to G_i\right\}_{i\in I}$ eine Familie von Homomorphismen, so gibt es genau einen Homomorphismus $\varphi: H \to G := \prod_{i\in I} G_i$ mit $\pi_i \circ \varphi = \varphi_i$. Dieser ist

$$\varphi(h) := \left(\varphi_i(h)\right)_{i\in I} \in G = \prod_{i\in I} G_i$$



10 **Definition: „direkte Summe“**

Die endliche Summe ist für eine Indexmenge I und eine Familie von Gruppen $\left\{G_i\right\}_{i\in I}$

$$\bigoplus_{i\in I} G_i := \left\{ \left(g_i\right)_{i\in I} \in \prod_{i\in I} G_i \;\middle|\; |\left\{ i \in I \mid g_i \neq e_i \right\}| < \infty \right\}$$

Die direkte Summe ist eine Untergruppe des direkten Produkts.

11 **Definition: „kanonische Injektionen“**

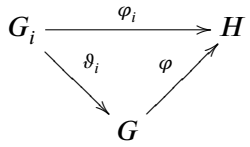
Die Abbildungen

$$\vartheta_j : G_j \to \bigoplus_{i\in I} G_i, \quad (\vartheta_j(g_j))_i = \begin{cases} g_j & i = j \\ e_i & i \neq j \end{cases}$$

nennen wir kanonische Injektionen.

12 **Satz: Universelle Eigenschaften der direkten Summe**

Sei $\left(G_i\right)_{i\in I}$ eine Familie von abelschen Gruppen und H eine abelsche Gruppe sowie $\varphi_i : G_i \to H$ eine Familie von Gruppenhomomorphismen. Dann gibt es genau einen Gruppenhomomorphismus $\varphi : G := \bigoplus_{i\in I} G_i \to H$ mit $\forall i \in I : \varphi \circ \vartheta_i = \varphi_i$



13 **Lemma: endlicher Fall**

Für $|I| < \infty$ ist

$$\bigoplus_{i\in I} G_i = \prod_{i\in I} G_i$$

14 **Definition: „Normalteiler“**

Sei $H \leq G$ eine Untergruppe, dann heißt sie Normalteiler wenn gilt:

$$\forall g \in G : g^{-1} H g \subseteq H$$

Wir schreiben $H \trianglelefteq G$.

15 **Definition: „Äquivalenzrelation“**

Für einen Normalteiler $H \trianglelefteq G$ definieren wir die Äquivalenzrelation

$$x, y \in G : x \equiv y \pmod{H} :\Leftrightarrow x^{-1} y \in H$$

16 **Definition: „Nebenklassen“**
Zu einem Normalteiler $H \trianglelefteq G$ sind die Linksnebenklassen

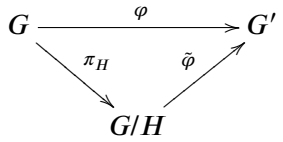
$$xH = \{ xh \mid h \in H \} \subseteq G$$

17 **Definition: „Faktorgruppe“**
Dann ergibt sich die Faktorgruppe als

$$G/H := \{ xH \mid x \in G \}$$
$$(xH)(yH) := (xy)H$$

18 **Definition: „kanonische Projektion“**
Die Abbildungen $\pi_H : G \to G/H$ mit $\pi_H(x) := xH$ heißen die kanonischen Projektionen von G auf die Faktorgruppe.

19 **Lemma: universelle Eigenschaft der Faktorgruppe**
Die Faktorgruppe G/H kann durch die folgende universelle Eigenschaft charakterisiert werden:
Es sei $\varphi: G \to G'$ ein Homomorphismus mit $H \leq \ker \varphi$. Dann existiert ein eindeutig bestimmter Gruppenhomomorphismus $\tilde{\varphi}: G/H \to G'$ mit $\tilde{\varphi} \circ \pi_H = \varphi$. Für $H = \ker \varphi$ ist $\tilde{\varphi}$ injektiv und $\operatorname{im} \tilde{\varphi} = \operatorname{im} \varphi$.



Beweis (19) Nach der Anforderung an $\tilde{\varphi}$ bleibt nur die eindeutige Definition

$$\tilde{\varphi}(xH) = \tilde{\varphi} \circ \varphi(x) := \varphi(x)$$

Da $H \leq \ker \varphi$ gilt $e' = \varphi(x^{-1}y) = \varphi(x)^{-1}\varphi(y)$ also $\varphi(x) = \varphi(y)$ für $xH = yH$.

20 **Korollar: Erster Isomorphiesatz**
Ist $\varphi: G \to G'$ ein Homomorphismus, dann gibt es einen Isomorphismus $\tilde{\varphi}: G/\ker \varphi \to \operatorname{im} \varphi$

21 **Lemma: Zweiter Isomorphiesatz**
Sei G eine Gruppe und $K \leq H \leq G$ und $K \trianglelefteq G$. Dann ist auch $K \trianglelefteq H$ und es gibt einen Isomorphismus

$$\frac{G/K}{H/K} \to G/H$$

Beweis (21) $K \trianglelefteq H$ folgt sofort aus der Definition des Normalteilers wegen $K \trianglelefteq G$ und $H \subseteq G$.
Wir wählen

$$\varphi: G/K \to G/H, \varphi(gK) := gH$$

Dies ist wohldefiniert und φ ist surjektiv. Dann ist $\ker \varphi = \{ gK \mid gH = H \} = H/K \leq G/K$. Nun folgt die Behauptung mit dem ersten Isomorphiesatz.

22 **Lemma: Dritter Isomorphiesatz**
Es seien $H \trianglelefteq G$ und $K \leq G$. Dann ist $(H \cap K) \trianglelefteq K$ und

$$K/(H \cap K) \simeq (HK)/H$$

Beweis (22) Da $H \trianglelefteq G$ gilt $(h_1k_1)(h_2k_2) = h_1 \underbrace{k_1h_2k_1^{-1}}_{\in H} k_1k_2 \in HK$ sowie $(hk)^{-1} = k^{-1}h^{-1} = \underbrace{k^{-1}h^{-1}k}_{\in H} k^{-1}$. Also ist $HK \leq G$. Dann sei $\varphi: K \to (HK)/H$ mit $\varphi(k) := kH$. φ ist surjektiv und $\ker \varphi = \{ k \in K \mid kH = H \} = \{ k \in K \mid k \in H \} = K \cap H$.

Beispiel

$G = \mathbb{Z}, H = 12\mathbb{Z}, K = 9\mathbb{Z}$
$H \cap K = 36\mathbb{Z}, HK = H + K = 3\mathbb{Z}$
$36\mathbb{Z} \leq 9\mathbb{Z}$
$\Rightarrow 9\mathbb{Z}/36\mathbb{Z} \simeq 3\mathbb{Z}/12\mathbb{Z}$

1.3 Aktionen von Gruppen

23 **Definition: „Aktion (Operation)“**
Eine Aktion (Operation) einer Gruppe G auf einer Menge X ist eine Abbildung

$$\varrho: G \times X \to X, \quad \varrho(g, x) = g \bullet x \in X$$

mit

1. $\forall g, h \in G, x \in X: \varrho(g, \varrho(h, x)) = \varrho(gh, x)$
2. $\forall x \in X: \varrho(e, x) = x$

Man sagt G operiert auf X.

Eine Aktion $\varrho: G \times X \to X$ definiert einen Homomorphismus $\bar{\varrho}: G \to S(X)$ durch $\bar{\varrho}(g)(x) = \varrho(g, x)$. Aus der Definition folgt dann $\bar{\varrho}(gh) = \bar{\varrho}(g)\bar{\varrho}(h)$ und $\bar{\varrho}(e) = Id_X$. Also ist $\bar{\varrho}(g^{-1}) = \bar{\varrho}(g)^{-1}$ — $\bar{\varrho}(g)$ ist bijektiv.
Diese Zuordnung von Aktionen und Homomorphismen $G \to S(X)$ gilt in beide Richtungen.

Beispiele

1. Sei G eine Gruppe, dann definieren wir die adjungierte symmetrische Darstellung von G

   $$ad: G \to \mathrm{Aut}(G), \quad ad(g)(x) := gxg^{-1}, \quad g \bullet x := gxg^{-1}$$

   Dann gilt

   $$g \bullet (h \bullet x) = g \bullet (hxh^{-1}) = g(hxh^{-1})g^{-1} = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = (gh) \bullet x$$
   $$e \bullet x = exe^{-1} = x$$

   Es handelt sich also um eine Aktion.

2. Linksmultiplikation

   $$l: G \to S(G), l(g)(x) = gx$$

   Dabei ist allerdings $l(G) \not\subseteq \mathrm{Aut}(G)$. Aber l ist eine Aktion.

3. Rechtsmultiplikation

   $$r: G \to S(G), r(g, x) := xg^{-1}$$

   Damit ergibt sich $ad = l \circ r = r \circ l$.

4. $$H = \{ z \in \mathbb{C} \mid \mathrm{Im}\, z > 0 \}$$
   $$SL_2(\mathbb{R}) \times H \to H, \gamma \bullet z = (az + b)(cz + d)^{-1}$$

24 **Definition: „Stabilisator“**
Ist ϱ eine Aktion einer Gruppe G auf X so ist der Stabilisator eines Elements $x \in X$:

$$\mathrm{Stab}_G(x) := \{ g \in G \mid g \bullet x = x \}$$

25 **Korollar: Eigenschaft des Stabilisators**
Der Stabilisator eines beliebigen Elements x ist eine Untergruppe von G.

26 **Definition: „Orbit“**
Für $x \in X$ heißt $G \bullet x := \{ g \bullet x \mid g \in G \}$ der Orbit (Bahn/Trajektorie) von x.

27 **Definition: „Kern einer Aktion“**
Der Kern einer Aktion ist

$$\ker \varrho := \ker \bar{\varrho} = \{ g \in G \mid \forall x \in X: g \bullet x = x \} = \bigcap_{x \in X} \mathrm{Stab}_G(x)$$

Damit ergibt sich eine Äquivalenzrelation auf X als

$$x_1 \sim x_2 :\Leftrightarrow \exists g \in G: x_2 = g \bullet x_1$$

nach der Definition einer Aktion. Die Äquivalenzklassen sind gerade die Orbits.

28 **Lemma: Klassengleichung**

$$\forall x \in X: |G \bullet x| = (G: \operatorname{Stab}_G(x))$$

Beweis (28) Wir definieren eine Abbildung

$$\psi: G \bullet x \to G/\operatorname{Stab}_G x: \psi(g \bullet x) = g \operatorname{Stab}_G x$$

Dann können wir folgern für $g_1, g_2 \in G$:

$$\begin{aligned} & g_1 \bullet x = g_2 \bullet x \\ \Leftrightarrow\ & (g_2^{-1} g_1) \bullet x = x \\ \Leftrightarrow\ & g_2^{-1} g_1 \in \operatorname{Stab}_G x \\ \Leftrightarrow\ & g_1 \operatorname{Stab}_G x = g_2 \operatorname{Stab}_G x \end{aligned}$$

Also ist ψ wohldefiniert und sogar bijektiv. □

Beispiele

1. Betrachten wir die Rechtsmultiplikation $r: G \times G \to G$, $r(g, x) = g \bullet x := xg^{-1}$ und ihre Beschränkung auf eine Untergruppe $H \leq G$: $r_H := r|_{H \times G}$. Dann ergeben sich als Orbit von $x = \left\{ r_H(h, x) = xh^{-1} \;\middle|\; h \in H \right\}$ die Linksnebenklassen xH. Mit der Klassengleichung erhalten wir dann $|G| = |G: H||xH| = |G: H||H|$ den Satz von Lagrange.

2. $\varrho: G \times G \to G$ mit $\varrho(g, x) := gxg^{-1}$ ist die Konjugationsoperation. Der Stabilisator ist hier der Zentralisator und wird als $C_G(x)$ bezeichnet. Dann ist $\ker \varrho = \bigcap_{x \in G} C_G(x)$ das Zentrum von G und es gilt auch

   $$x \in Z(G) \Leftrightarrow G \bullet x = \{x\}$$

   Die Klassengleichung ergibt sich als

   $$|G| = \sum_{G \bullet x} |G \bullet x| = |Z(G)| + \sum_{C_G(x) \neq G} (G: C_G(x))$$

3. Sei $H \leq G$ und $\alpha: G \times (G/H)_{\text{links}} \to (G/H)_{\text{links}}$ mit $\alpha(g, xH) = gxH$ eine Aktion auf den Linksnebenklassen bzgl. H. Es ergibt sich

   $$\begin{aligned} & H_G := \ker \alpha = \{\, g \in G \mid \forall x \in G: gxH = xH \,\} \\ & = \left\{ g \in G \;\middle|\; \forall x \in G: x^{-1} g x \in H \right\} = \left\{ g \in G \;\middle|\; \forall x \in G: g \in xHx^{-1} \right\} \\ & = \bigcap_{x \in G} xHx^{-1} \trianglelefteq G \\ & H_G \leq H \end{aligned}$$

29 **Lemma:**

H_G ist der größte Normalteiler von G in H ist.

30 **Satz: Satz von Cauchy**

Sei G eine endliche Gruppe und p ein Primteiler der Ordnung $|G|$. Dann besitzt G ein Element $x \in G$ mit $|x|_G = p$.

Beweis (30) Wir wählen p fest und führen eine Induktion nach der Ordnung von G durch.

$$|G| = p \Rightarrow G \simeq \mathbb{Z}_p = \langle \bar{1} \rangle, \quad |\bar{1}|_G = p$$

Setzt man voraus, dass G abelsch ist

1. Wenn G keine nicht-triviale Untergruppe besitzt $\Rightarrow G$ ist zyklisch $1 \neq x \in G: \langle x \rangle \leq G \Rightarrow G = \langle x \rangle: |G| = n$ und $|G| = p$, $G \simeq \mathbb{Z}_p$
   $G \simeq \mathbb{Z}$, $n = pq$ $\langle \bar{0}, \bar{p}, \bar{2p}, \cdots, (q + \bar{p}) \rangle \leq G$
2. wenn G nicht-triviale Untergruppe besitzt $\Rightarrow \exists s: H \leq G$
   $\{1\} \neq H, H \neq G$
   $p \mid |G| = |H||G: H| \Rightarrow p \mid |H|$ Wenn $p \mid |H|$ und $|H| < |G| \Rightarrow \exists x \in H: p \mid |G: H|$ $|x|_G = p$✓ $\neg p \mid |H|$. Setzen $m = |H|$ ggT$(p, m) = 1$ $p \mid |G/H| \Rightarrow \exists s: xH \in G/H, |xH|_{G/H} = p$ $(xH)^p = H \Leftrightarrow x^p H = H \Leftrightarrow x^p \in H$ Setzt man $y = x^{mn} \in G$ $y^p = x^{mnp} = ((x^p)^n)^m = 1 \Rightarrow |y|_G \mid p$ Zu zeigen: $y = 1$ $y = 1 \Leftrightarrow x^{mn} = 1 \Rightarrow \underbrace{|xH|_{G/H}}_{p} \mid mn \Rightarrow p \mid mn \Rightarrow p \mid 1$ ↯

Ist G nicht unbedingt abelsch, betrachtet man die Klassengleichung für die Konjugation ϱ auf G. Dabei ist dann

$$\begin{aligned}
&\mathrm{Stab}_G(x) = \{\, g \in G \mid gx = xg \,\} = C_G(x) \\
&Gx = \left\{\, gxg^{-1} \;\middle|\; g \in G \,\right\} \\
&Gx = \{x\} \Leftrightarrow C_G(x) = G \Leftrightarrow x \in Z(G) \\
&\Longrightarrow |G| = |Z(G)| + \sum_{Gx \neq \{x\}} (G: C_G(x))
\end{aligned}$$

- Falls $p \mid |Z(G)| \Rightarrow \exists x \in Z(G) \subset G: |x|_G = p$
- Sonst $\exists x \in G: Gx \neq \{x\}$, sodass $p \nmid |G: C_G(x)| \wedge p \mid |G| \Rightarrow p \mid |C_G(x)| \wedge C_G(x) < G \xRightarrow{\text{Induktion}} |G| = |G: C_G(x)||C_G(x)| \Rightarrow \exists y \in C_G(x): |y|_{C_G} = p$ □

31 **Definition: „p-Gruppe“**

Ist G eine Gruppe und $|G| = p^m, p \in \mathbb{P}, m \geq 1$, so heißt G p-Gruppe.

32 **Definition: „p-Sylow-Untergruppe“**

Eine Untergruppe von G heißt p-Sylow-Untergruppe, wenn ihre Ordnung p^m und die Potenz von p in $|G|$ genau m ist.

33 **Definition: „Fixpunkte“**

$\mathrm{Fix}_G(X)$ bezeichne die Fixpunkte in X unter einer Operation von G.

34 **Lemma: Anzahl an Fixpunkten**

Sei G eine p-Gruppe, X endlich und ϱ eine Operation von G auf X, dann gilt

$$|\mathrm{Fix}_G(X)| \equiv |X| \mod p$$

Beweis (34) Die Klassengleichung für ϱ lautet

$$|X| = |\mathrm{Fix}_G(X)| + \sum_{Gx \neq \{x\}} (G\colon \mathrm{Stab}_G(x))$$

$$Gx \neq \{x\} \Leftrightarrow \mathrm{Stab}_G(x) \neq G$$
$$\mathrm{Stab}_G(x) \neq G \Rightarrow p \mid (G\colon \mathrm{Stab}_G(x))$$
$$\Rightarrow |X| \equiv |\mathrm{Fix}_G(X)| \mod p$$

□

35 **Definition: „Normalisator“**

Der Normalisator von $H \leq G$ in G ist die größte Untergruppe $N_G(H) \leq G$, sodass $H \trianglelefteq N_G(H)$. Das heißt

$$H \trianglelefteq N_G(H) \leq G$$
$$H \trianglelefteq k \leq G \Rightarrow k \leq N_G(H)$$

Oder anders:

$$N_G(H) := \{\, g \in G \mid gH = Hg \,\}$$

bzw.

$$\alpha\colon G \times \mathcal{P}(G) \to \mathcal{P}(G), \alpha(g, U) = gUg^{-1} \Rightarrow N_G(H) = \mathrm{Stab}^{\alpha}_G(H)$$

36 **Lemma: Primteiler vom Index des Normalisators**

Sei G eine endliche Gruppe und H eine p-Untergruppe von G mit $p \mid (G\colon H)$, dann gilt $p \mid (N_G(H)\colon H)$.

Beweis (36) Sei ρ die Aktion G auf den Linksnebenklassen von H mittels Linksmultiplikation, dann gilt nach dem Lemma 34:

$$(G\colon H) = |(G/H)_{\text{links}}| \equiv |\mathrm{Fix}_H\left((G/H)_{\text{links}}\right)| \mod p$$

wobei $\mathrm{Fix}_H\left((G/H)_{\text{links}}\right) = N_G(H)/H$, also

$$(G\colon H) \equiv (N_G(H)\colon H) \mod p$$ □

37 **Satz: Erster Satz von Sylow**

Sei G eine endliche Gruppe und $p \mid |G|$. Dann hat G eine p-Sylow-Untergruppe.

Beweis (37) Wir wissen, nach dem Satz von Cauchy, dass es eine Untergruppe der Ordnung p gibt. Sei H eine p-Untergruppe der Ordnung p^m. Dann ist sie entweder bereits p-Sylow oder $p \mid (G\colon H)$. Das bedeutet nach dem obigen Lemma $p \mid (N_G(H)\colon H)$. Dann gibt es wiederum nach dem Satz von Cauchy ein Element $x \in N_G(H)/H$ mit $|x|_{N_G(H)/H} = p$ und

$$\begin{aligned}\langle x\rangle \quad &= K/H, \qquad H \leq K \leq N_G(H) \leq G\\ \Rightarrow |K| &= |H|(K\colon H) = p^{m+1}\end{aligned}$$

Da G endlich ist, gibt es also eine p-Sylow-Untergruppe.

38 **Satz: Zweiter Satz von Sylow**

Es sei p ein Primteiler von $|G|$, K eine p-Untergruppe und H eine p-Sylow-Untergruppe von G. Dann gibt es ein $g \in G$ mit $K \leq gHg^{-1}$. Insbesondere sind alle p-Sylow-Untergruppen zueinander konjugiert sind.

Beweis (38) Sei α die Aktion von K auf den Linksnebenklassen von H in G mittels Linksmultiplikation. Dann ist

$$(G\colon H) \equiv |\mathrm{Fix}_K\left((G/H)_{\text{links}}\right)| \mod p$$

Da p kein Teiler von $(G\colon H)$ ist, gibt es also mindestens einen Fixpunkt, sodass $kgH = gH$ also $K \leq gHg^{-1}$.

39 **Definition: „Anzahl der p-Sylow-Untergruppen“**

Die Anzahl der p-Sylow-Untergruppen für ein bestimmtes $p \in \mathbb{P}$ ist

$$n_p := \#\{\ H \leq G \mid H \text{ ist eine p-Sylow-Untergruppe von } G\ \} =: \#S_p$$

40 **Satz: Dritter Satz von Sylow**

Für die Anzahl der p-Sylow-Untergruppen einer endlichen Gruppe G gilt:

1. $n_p = \left(G\colon N_G(H)\right)$

2. $n_p \mid (G: H)$
3. $n_p \equiv 1 \mod p$

wenn H eine p-Sylow-Untergruppe von G ist.

Beweis (40)

1. Nach dem zweiten Satz von Sylow gilt

$$\begin{aligned} &S_p = \left\{ gHg^{-1} \;\middle|\; g \in G \right\} = G \bullet H \\ &\Rightarrow |S_p| = (G: \mathrm{Stab}_G(H)) = (G: N_G(H)) \\ &\Rightarrow n_p = (G: N_G(H)) \end{aligned}$$

2. Weiter ist $H \leq N_G(H) \leq G$, also gilt nach dem Satz von Lagrange

$$(G: H) = (G: N_G(H))(N_G(H): H)$$

Woraus man die zweite Behauptung sofort ablesen kann.

3. Auf der Menge S_p operiert H durch Konjugation.

$$\alpha: H \times S_p \to S_p, \quad \alpha(h, P) = hPh^{-1}$$

Nach dem Lemma 34 gilt dann

$$n_p = |S_p| \equiv |\mathrm{Fix}_H(S_p)| \mod p$$

Dabei ist nun

$$\begin{aligned} &\mathrm{Fix}_H(S_p) = \left\{ P \in S_p \;\middle|\; \forall h \in H: hPh^{-1} = P \right\} \\ &= \left\{ P \in S_p \;\middle|\; \forall h \in H: h \in N_G(P) \right\} \\ &= \left\{ P \in S_p \;\middle|\; H \leq N_G(P) \right\} = \{H\} \end{aligned}$$

(Dabei sei auf Übung 4.4.1 verwiesen.)

Also gilt auch diese Behauptung.

41 **Definition: „einfache Gruppen“**
Eine Gruppe mit genau zwei Normalteilern heißt einfach.

1.4 Gruppen von Ordnung pq

42 **Satz: Satz 1**
Es gibt keine einfache Gruppe der Ordnung pq, $p \neq q$.

Beweis (42) Sei P eine p-Sylow-Untergruppe von G, dann ist $|P| = p$, also $P = \langle x \rangle$ zyklisch. Analog für $Q(q)$. Außerdem gilt

$$n_p \mid (G\colon P) \Rightarrow n_p \mid q \Rightarrow n_p \in \{1, q\}$$

bzw. $n_q \in \{1, p\}$. Nach dem dritten Satz von Sylow kann nicht $n_p = q$ und gleichzeitig $n_q = p$ sein, da $q \equiv 1 \mod p \wedge p \equiv 1 \mod q$ ein Widerspruch ist. Also ist oBdA $n_p = 1 \Leftrightarrow N_G(P) = G \Leftrightarrow P \lhd G$: G ist nicht einfach.

43 **Satz: Satz 2**

Seien $p, q \in \mathbb{P}$ und $p \not\equiv 1 \mod q$ sowie $q \not\equiv 1 \mod p$. Dann ist G zyklisch, sodass $G \simeq \mathbb{Z}/(pq\mathbb{Z})$.

Beweis (43) Wir wissen sofort dass $n_p = n_q = 1$, also $P \lhd G$ und $Q \lhd G$. Wenn $P = \langle x \rangle$ und $Q = \langle y \rangle$ ist, dann folgt $xyx^{-1}y^{-1} \in P \cap Q = \{1\}$. Also ist $xy = yx$. Wir wissen weiterhin, dass $|xy|_G = pq$. Sei $n := |xy|_G$. Dann folgt

$$\begin{aligned}
&(xy)^n = 1 \Rightarrow x^n y^n = 1 \\
&\Rightarrow x^n = y^{-n} \in P \cap Q = \{1\} \\
&\Rightarrow x^n = y^n = 1 \Rightarrow |x|_G = p \mid n \wedge |y|_G = q \mid n \\
&\Rightarrow n = pq \wedge |xy|_G = |G|
\end{aligned}$$

G ist also zyklisch.

1.5 Die Permutationsgruppe

44 **Definition: „Permutation“**

Wir definieren mit $[n] := \{1, 2, \cdots, n\}$ eine Aktion

$$\begin{aligned}
&S_n \times [n] \to [n] \\
&(\sigma, x) \mapsto \sigma \bullet x := \sigma(x)
\end{aligned}$$

Dann ist der Stabilisator

$$\mathrm{Stab}_{S_n}(x) = \left\{ \sigma \in S_n \mid \sigma(x) = x \right\} \simeq S_{n-1} \leq S_n$$

45 **Definition: „Zykel“**

Ein Zykel $\nu \in S_n$ ist durch eine Teilmenge $T = \left\{t_1, \cdots, t_l\right\} \subseteq [n]$ gegeben, sodass $\mu(t_1) = t_2, \mu(t_2) = t_3, \cdots, \mu(t_{l-1}) = t_l, \mu(t_l) = t_1$ und $\mu(t) = t$ für $t \notin T$. Dabei heißt l die Länge des Zykels und T die Bahn des Zykels.

46 **Bemerkung: Eigenschaften von Zykeln**

- $|\mu|_{S_n} = l$
- Zwei Zykel mit disjunkten Bahnen kommutieren

- Jede Permutation kann als Produkts von Zykeln dargestellt werden. (Diese können beispielsweise durch disjunkte Zerlegung der Orbits gefunden werden.)
- Jeder Zykel (und damit jede Permutation) kann als Produkt von Transpositionen geschrieben werden.

47 **Lemma: Konjugation**

Ist $\sigma = \begin{pmatrix} m & \sigma(m) & \cdots & \sigma^{l-1}(m) \end{pmatrix}$ ein Zykel der Länge l und $\tau \in S_n$ beliebig. Dann ist $\tau\sigma\tau^{-1}$ ein Zykel und es gilt

$$\tau\sigma\tau^{-1} = \begin{pmatrix} \tau(m) & \tau\sigma(m) & \cdots & \tau\sigma^{l-1}(m) \end{pmatrix}$$

48 **Satz: Konjugationsklassen**

Konjugationsklassen in S_n entsprechen Partitionen von n.

Beweis (48) Dies gilt, da die Partitionen den eindeutigen Zerlegungen in disjunkte Orbite zugeordnet werden können und alle Permutationen mit gleichgroßen disjunkten Orbiten konjugiert sind, denn Konjugation bedeutet die entsprechende Umbenennung nach dem vorherigen Lemma.

49 **Definition: „Signum“**

Das Signum/Vorzeichen einer Permutation ist

$$\operatorname{sgn}\sigma := -1^{|\{\ (i<j)\ |\ \sigma(i)>\sigma(j)\ \}|}$$

Dabei gilt

$$\operatorname{sgn}\sigma = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$$

und sgn ist ein Gruppenhomomorphismus von S_n in $\{+1, -1\} \simeq \mathbb{Z}_2$.

50 **Definition: „Die alternierende Gruppe“**

Die alterniere Gruppe A_n ist definiert als:

$$A_n := \ker(\operatorname{sgn}) = \left\{ \sigma \in S_n \;\middle|\; \operatorname{sgn}(\sigma) = +1 \right\} \trianglelefteq S_n$$

51 **Lemma: Konjugationsklassen der alternierenden Gruppe**

Sei $\sigma \in A_n$. Gibt es eine Transposition $\tau \in S_n$, die mit σ kommutiert, dann sind die Konjugationsklassen von σ in A_n und S_n gleich. ($A_n\sigma = S_n\sigma$ für die Konjugationsaktion)

52 **Satz: Einfache alternierende Gruppen**

Alle alternierenden Gruppen A_n mit $n \geq 5$ sind einfach.

Beweis (52) Wir führen den Beweis per Induktion. Für A_5 ist die Einfachheit bekannt. Angenommen A_n ist einfach für $n \geq 5$. Wir betrachten die Stabilisatoruntergruppen von A_{n+1}:

$$H_i := \mathrm{Stab}_{A_{n+1}}(i) = \left\{ \sigma \in A_{n+1} \;\middle|\; \sigma(i) = i \right\}$$

Dann ist per Projektion auf $\{1, \cdots, n\}$ die Untergruppe $H_{n+1} \simeq A_n$. Analog kann man für ein beliebiges i eine Bijektion finden, die $H_i \simeq A_n$ ergibt. Alternativ kann man auch zeigen, dass alle H_i und H_j in A_{n+1} konjugiert sind. Gibt es nun einen Normalteiler $K \trianglelefteq A_{n+1}$, so ist $K \cap H_i \trianglelefteq H_i$. Jedoch ist H_i einfach und somit gilt entweder $K \cap H_i = \{Id\}$ oder $K \cap H_i = H_i \Leftrightarrow H_i \subseteq K$.

- Angenommen es gibt ein $H_j \subseteq K$, dann gilt auch für alle anderen $H_i = \tau H_j \tau^{-1} \subset \tau K \tau^{-1} = K$. Dies bedeutet jedoch $K = A_{n+1}$.
- Gilt dagegen für alle i, dass $H_i \cap K = \{Id\}$, so erfüllt jedes $\sigma \in K$ die Bedingung $\sigma(i) \neq i$. Wählen wir nun ein festes Element $a \in \{1, \cdots, n+1\}$. Dazu können wir wegen $n \geq 5$ weitere Elemente finden, sodass wir die Menge $\{a, b, c, d, e, f\}$ mit $b = \sigma(a)$, $d = \sigma(c)$ erhalten. Nun betrachten wir $\tau := (ab)(cdef) \in A_{n+1}$. Dabei erhalten wir

  $$(\tau\sigma\tau^{-1})(b) = \tau\sigma(\tau^{-1}(b)) = \tau\sigma(a) = \tau(b) = a$$
  $$(\tau\sigma\tau^{-1})(d) = \tau\sigma(\tau^{-1}(d)) = \tau\sigma(c) = \tau(d) = e$$
  $$\tau\sigma\tau^{-1}\sigma(a) = \tau\sigma\tau^{-1}(b) = a\tau\sigma\tau^{-1}\sigma(e) \neq \tau\sigma\tau^{-1}(d) = e$$

  Dies ist ein Widerspruch.

53 **Bemerkung:**
Die alternierende Gruppe A_5 ist bis auf Isomorphie die einzige nicht abelsche einfache Gruppe von Ordnung kleiner gleich 100.

2 Ringtheorie

2.1 Wiederholung

54 **Definition: „Ring“**
Eine Menge R mit zwei Operationen $+: R \times R \to R$ und $\cdot: R \times R \to R$ heißt Ring, wenn die folgenden Eigenschaften gelten:

1. $(R, +)$ ist eine abelsche Gruppe
2. $\forall x, y, z \in R: x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (Assoziativität)
3. $\forall x, y, z \in R: (x + y) \cdot z = x \cdot z + y \cdot z \wedge x \cdot (y + z) = x \cdot y + x \cdot z$ (Distributivität)

Gilt zusätzlich $x \cdot y = y \cdot x$, so ist R ein kommutativer Ring. Falls $\exists \mathbf{1} \in R: x \cdot \mathbf{1} = \mathbf{1} \cdot x = x$, so heißt R unitärer Ring.

Beispiele

1. Die quadratischen Matrizen $K^{n\times n}$ mit elementweiser Addition und Matrixmultiplikation bilden einen nicht-kommutativen Ring.
2. Die Endomorphismen einer abelschen Gruppe bilden ebenfalls einen nicht-kommutativen Ring mittels Gruppenoperation und Verkettung.

55 **Definition: „Unterring“**
Eine Menge $R' \subseteq R$ heißt Unterring, falls $(R', +) \leq (R, +)$ und $\forall x, y \in R' : x \cdot y \in R'$.

56 **Definition: „Ideal“**
Eine Menge $I \subseteq R$ heißt Linksideal, falls

1. $(I, +) \leq (R, +)$
2. $R \cdot I \subseteq I$, d.h. $\forall x \in R, a \in I : x \cdot a \in I$

Für ein Rechtsideal muss dagegen $I \cdot R \subseteq I$ sein.
Ist I sowohl Links- als auch Rechtsideal, so heißt es zweiseitiges Ideal.

57 **Bemerkung: kommutative Ringe**
In kommutativen Ringen sind alle diese Formen von Idealen gleichbedeutend.

Beispiele

1. $\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$, jedoch kein Ideal.
2. In Z_n sind alle Untergruppen auch Unterringe und Ideale.

58 **Definition: „Hauptideal“**
Für ein beliebiges Element $a \in R$ heißt $Ra := \{ ra \mid r \in R \}$ das von a erzeugte Linkshauptideal. (Rechtshauptideal analog)
Das zweiseitige Hauptideal ist $RaR := \{ sar \mid s, r \in R \}$.
Alle Hauptideale sind Ideale.

59 **Definition: „Ideal von Untermengen“**
Das von einer Menge $A \subset R$ erzeugte (Links-, Rechts- oder zweiseitge) Ideal ist das kleinste Ideal $I \subseteq R$ mit $A \subseteq I$:

$$I = \bigcap \{ \text{ Ideal } J \mid A \subseteq J \subseteq R \}$$

60 **Lemma: Berechnung von Idealen**

Das von $A \subseteq R$ erzeugte Linksideal kann als

$$I = \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; n \in \mathbb{N}, a_i \in R, x_i \in A \right\}$$

dargestellt werden.

61 **Definition: „Ringhomomorphismus“**

Ein Ringhomomorphismus ist eine Abbildung f von einem Ring $(R, +, \cdot)$ in einen zweiten Ring $(S, \times, \bullet)$ mit $f(x \cdot y) = f(x) \bullet f(y)$ und $f(x + y) = f(x) \times f(y)$. (Jeder Ringhomomorphismus ist also auch ein Gruppenhomomorphismus) Ist R unitär, so muss auch $f(R)$ unitär sein (S dagegen nicht unbedingt) und $f(\mathbf{1}_R)$ ist ein Einselement in $f(R)$.

62 **Lemma: Kern des Ringhomomorphismus**

Ist $f: R \to S$ ein Ringhomomorphismus, so ist $\ker(f) \subset R$ ein zweiseitiges Ideal und ein Unterring.

63 **Definition: „Quotientengruppe“**

Sei I ein Ideal und eine Untergruppe von einem Ring R, dann ist die Quotientengruppe definiert als

$$R/I := \{\, a + I \mid a \in R \,\}$$

64 **Satz: Quotientenringe**

Falls I ein zweiseitiges Ideal in R ist, ist R/I ein Ring und die Projektion $\pi: R \to R/I, \quad a \mapsto a + I$ ein Ringhomomorphismus.

65 **Lemma:**

Ist $I \subseteq R$ ein zweiseitiges Ideal und $\varphi: R \to S$ ein Ringhomomorphismus mit $I \subseteq \ker(\varphi)$. Dann existiert ein eindeutiger Ringhomomorphismus $\tilde{\varphi}: R/I \to S$ mit $\varphi = \tilde{\varphi} \circ \pi$.

66 **Definition: „Primideal“**

Ein Ideal $p \subset R$ heißt Primideal genau dann, wenn

$$\forall a, b \in R: a \cdot b \in p \Rightarrow a \in p \vee b \in p$$

67 **Bemerkung: Verallgemeinerung**

Der Begriff des Primideals ist eine Verallgemeinerung der Primzahlen, denn ein Hauptideal $p\mathbb{Z}$ ist genau dann ein Primideal, wenn $p = 0$ oder prim ist. Die Idee der Teilbarkeit in $\mathbb{Z}$ entpricht in Ringen dem Begriff der Inklusion von Idealen.

68 **Definition: „Nullteiler, nilpotent, Integritätsbereich“**

Ein Element $x \in R \setminus \{0\}$ heißt Nullteiler, wenn es ein $y \neq 0$ gibt mit $x \cdot y = 0$. Es heißt nilpotent, wenn es ein $n \in \mathbb{N} \setminus \{0\}$ gibt mit $x^n = 0$. Ein unitärer Ring ohne Nullteiler heißt auch Integritätsbereich.

69 **Satz: Primideale und Integritätsbereiche**

Ein Ideal $p \subset R$ ist genau dann ein Primideal, wenn R/p ein Integritätsbereich ist.

70 **Definition: „Einheit, Körper“**

Ein Element eines unitären Ringes heißt Einheit, wenn es ein Inverses bezügliches der Ringmultiplikation gibt.

Sind alle Elemente bis auf das Nullelement Einheiten, so heißt der Ring auch Körper.

71 **Lemma: maximale Ideale**

Ein Ideal in R ist genau dann maximal, wenn es in keinem Ideal außer R echt enthalten ist.

1. Ein Ring ist genau dann ein Körper, wenn er keine nicht-trivialen Ideale besitzt.
2. Ein Ideal $I \subset R$ ist genau dann maximal, wenn R/I ein Körper ist.

2.2 kommutative, unitäre Ringe

72 **Lemma: über maximale Ideale**

Sei R ein kommutativer unitärer Ring und m ein echtes Ideal von R, dann sind die folgenden Aussagen äquivalent:

1. m ist ein maximales Ideal
2. $\forall a \in R \setminus m: m + (a) = R$
3. R/m ist ein Körper

Beweis (72)

1. $\Rightarrow$ 2. Ist $a \in R$, so ist $I := m + (a) = \{ x + ra \mid x \in m, r \in R \}$ ein Ideal, dass m enthält. Wenn aber m ein maximales Ideal ist, so muss $I = R$ sein.

2. $\Rightarrow$ 3. Es gilt

$$\begin{aligned}
&\bar{0} \neq \bar{a} \in R/m \Leftrightarrow a \in R \setminus m \Rightarrow m + (a) = R \\
&\Rightarrow \mathbf{1} \in m + (a) \Rightarrow \exists x \in m, \lambda \in R: \mathbf{1} = x + \lambda a \\
&\Rightarrow \bar{\mathbf{1}} = \bar{x} + \bar{\lambda}\bar{a} \quad \text{in } R/m \\
&\overset{x \in m}{\Longrightarrow} \bar{\mathbf{1}} = \bar{\lambda}\bar{a} \text{ invertierbar}
\end{aligned}$$

Also ist R/m ein Körper.

3. $\Rightarrow$ 1. Haben wir bereits in Lemma 71 gezeigt.

2.2.1 Das Zornsche Lemma

73 **Definition: „Ordnungsrelation“**

Sei M eine Menge. Eine Relation $\leq$ auf M ist eine Teilmenge von $M \times M$.
$\leq$ heißt Ordnungsrelation, falls für alle $x, y, z \in M$ gilt:

Reflexivität $x \leq x$

Transitivität $x \leq y \wedge y \leq z \Rightarrow x \leq z$

Antisymmetrie $x \leq y \wedge y \leq x \Rightarrow x = y$

Man bezeichnet dann $(M, \leq)$ als geordnete Menge. Gilt zusätzlich für jedes Paar $x, y \in M$ entweder $x \leq y$ oder $y \leq x$, so heißt $(M, \leq)$ sogar total geordnet.

74 **Definition: „Maximalität“**

Ist $\leq$ eine Ordnungsrelation auf M, so heißt ein Element $m \in M$ genau dann maximal, wenn für alle $x \in M$ gilt $m \leq x \Rightarrow x = m$.

75 **Definition: „obere Schranke“**

Sei $S \subseteq M$, dann heißt ein Element $m \in M$ obere Schranke von S gdw. $\forall s \in S: s \leq m$ gilt.

76 **Satz: Zornsches Lemma**

Sei $(M, \leq)$ eine geordnete Menge in der jede totalgeordnete Teilmenge $S \subseteq M$ eine obere Schranke besitzt. Dann existiert in M ein maximales Element.

77 **Satz: Existenzsatz über maximale Ideale**

Sei R ein kommutativer Ring und $I \subsetneq R$ ein Ideal. Dann ist I in einem maximalen Ideal enthalten.

Beweis (77) Wir definieren

$$\mathcal{P} := \{ \text{ Ideal } J \mid I \subseteq J \subsetneq R \}$$

und wählen die Teilmengenbeziehung als Ordnung. Um nun das Zornsche Lemma anzuwenden, müssen wir zeigen, dass jede totalgeordnete Teilmenge von $\mathcal{P}$ eine obere Schranke hat.

Sei $\{J_\alpha\}_{\alpha \in A}$ die Familie der totalgeordneten Ideale in $\mathcal{P}$. Dann setzen wir

$$J := \bigcup_{\alpha \in A} J_\alpha \subseteq R$$

Wie man bald sieht, ist J ein Ideal in R. Sei $x, y \in J$, dann ist oBdA $x \in J_\alpha$ und $y \in J_\beta$ sowie $J_\alpha \subseteq J_\beta$. Damit gilt aber auch $x \in J_\beta$, also $x - y \in J_\beta \subseteq J$. Weiter gilt für $x \in J$, $x \in J_\alpha \Rightarrow ax \in J_\alpha \subseteq J$. Somit ist J eine obere Schranke für jede totalgeordnete Menge aus $\mathcal{P}$. Außerdem kann J nicht gleich R sein, da dann eine der Mengen J_α die $\mathbf{1}$ enthalten muss, was nicht möglich ist, da alle J_α nicht gleich R sind.

Nach dem Lemma von Zorn gibt es also ein maximales Element in $\mathcal{P}$. □

78 **Korollar:**
Jedes nichtinvertiertbare Element in einem Ring ist in einem maximalen Ideal enthalten.

79 **Definition: „lokaler Ring“**
Ein kommutativer Ring R mit nur einem maximalen Ideal $m \subseteq R$ heißt lokaler Ring.

80 **Bemerkung:**
Körper sind lokale Ringe, denn das einzige maximale Ideal ist $\{0\}$.

81 **Definition: „Menge der Einheiten“**
Die Mengen der Einheiten eines Ringes R bezeichnen wir als $U(R)$.

82 **Lemma: Charakterisierung lokaler Ringe**
Sei R ein kommutativer Ring, so sind die folgenden Aussagen äquivalent:

1. R ist ein lokaler Ring
2. Falls $a, b \in R$ mit $a + b = \mathbf{1}$ so ist $a \in U(R) \vee b \in U(R)$.
3. $R \setminus U(R)$ ist ein Ideal (das maximale Ideal)

2.3 Lokalisierung

Im folgenden wollen wir aus einer Teilmenge $S \subseteq R$ eines Ringes R den Ring der Quotienten $S^{-1}R = \left\{ \frac{a}{s} : a \in R, s \in S \right\}$ konstruieren. An dieser Stelle ist jedoch noch offen, was $\frac{a}{s}$ bedeuten soll.

83 **Definition: „multiplikative Teilmenge“**
Eine Teilmenge $S \subseteq R$ heißt multiplikativ, wenn folgendes erfüllt ist:

1. $0 \notin S, \mathbf{1} \in S$
2. $\forall a, b \in S: a \cdot b \in S$

Beispiele

1. $S = \{\mathbf{1}\}$
2. $a \in S$ beliebig: $S = \{\ a^n \mid n \geq 0\ \}$
3. $S = U(R)$
4. $R \setminus p$ wobei p ein Primideal ist.

Auf der Menge $R \times S$ betrachten wir die folgende Äquivalenzrelation:

$$(a, s) \sim (b, t) :\Leftrightarrow \exists x \in S: x(at - bs) = 0$$

Einzig interessant ist hier die Transitivität:

$$\begin{aligned}
&x(at - bs) = 0 \wedge y(bu - ct) = 0 \\
&\Leftrightarrow xat = xbs \wedge ybu = yct \\
&\Rightarrow xyatu = xybsu \wedge xybsu = xycst \\
&\Rightarrow (xyt)(au) = (xyt)(cs) \Rightarrow xyt(au - cs) = 0 \\
&\overset{xyt \in S}{\Longrightarrow} (a, s) \sim (c, u)
\end{aligned}$$

Nun bezeichnen wir mit $\frac{a}{s}$ die Äquivalenzklasse von (a, s). Das heißt

$$\frac{a}{s} = \frac{b}{t} \Leftrightarrow \exists x \in S: x(at - bs) = 0$$

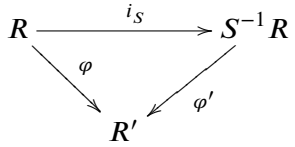
Damit wird die obige Definition von $S^{-1}R$ ergänzt.

84 **Lemma:**
$S^{-1}R$ ist ein Ring mit den folgenden Operationen:

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st}$$
$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}$$

Es ist offensichtlich, dass diese Operationen wohldefiniert sind und wirklich einen Ring bilden.
Die Projektion $i_S: R \to S^{-1}R, \quad i_S(a) \mapsto \frac{a}{1}$ ist nun ein Ringhomomorphismus. Weiter gilt dann $i_S(S) \subseteq U(S^{-1}R)$. Für einen Integritätsbereich R ist i_S außerdem immer injektiv.

85 **Lemma: Universelle Eigenschaft der Lokalisierung**
Ist $S \subseteq R$ eine multiplikative Teilmenge und $\varphi: R \to R'$ ein Ringhomomorphismus mit $\varphi(S) \subseteq U(R')$. Dann gibt es einen eindeutig bestimmten Homomorphismus $\varphi': S^{-1}R \to R'$ mit $\varphi' \circ i_S = \varphi$.



Beispiele

1. Ist R ein Integritätsbereich, so ist $S = R \setminus \{0\}$ die maximale multiplikative Menge und $S^{-1}R =: Q(R)$ ist der Quotientenkörper von R. Insbesondere bei $R = \mathbb{Z}$ ist $Q(\mathbb{Z}) = \mathbb{Q}$.
2. Ist $p \subseteq R$ ein Primideal, so ist bekanntlich $S := R \setminus p$ eine multiplikative Menge. Wir bezeichnen dann $S^{-1}R$ mit R_p den lokalisierten Ring.

2.4 Hauptideale und faktorielle Ringe

Im folgenden betrachten wir immer R als Integritätsbereich.

86 **Definition: „Teilbarkeit“**

Seien $a, b \in R$, dann sagen wir a teilt b ($a \mid b$) und a ist ein Teiler von b, wenn es ein $r \in R$ gibt mit $b = ra$.

87 **Lemma: Eigenschaften der Teilbarkeit**

Für $a, b \in R$ gilt:

1. $a \mid b \Leftrightarrow (b) \subseteq (a) \Leftrightarrow Rb \subseteq Ra$
2. $a \mid a,\ a \mid b \wedge b \mid c \Rightarrow a \mid c$
3. $a \mid b \wedge b \mid a \Leftrightarrow \exists r \in U(R)\colon b = ra$

88 **Definition: „Assoziation“**

Nun können wir also eine Relation definieren:

$$a \sim b :\Leftrightarrow Ra = Rb \Leftrightarrow b = \lambda a, \lambda \in U(R)$$

Wir sagen a und b sind assoziiert.

89 **Definition: „größter gemeinsamer Teiler“**

Seien $a, b \in R \setminus \{0\}$, dann heißt ein $d \in R$ mit $d \mid a \wedge d \mid b$ heißt gemeinsamer Teiler von a und b. d ist der größter gemeinsamer Teiler, wenn alle gemeinsamen Teiler von a und b auch d teilen. (Bezeichnung $d = \mathrm{ggT}(a, b)$ bzw. $d = gcd(a, b)$.) Zwar ist der größte gemeinsame Teiler nicht eindeutig bestimmt, jedoch sind alle größten gemeinsamen Teiler von a und b assoziiert.

90 **Definition: „kleinstes gemeinsames Vielfaches“**

Seien a, b wiederum aus $R \setminus \{0\}$. Jetzt heißt $m \in R$ ein gemeinsames Vielfaches von a und b, wenn $a \mid m \wedge b \mid m$. Teilt m alle gemeinsamen Vielfachen von a und b, so heißt es ein kleinstes gemeinsames Vielfaches. (Wir schreiben $m = \mathrm{kgV}(a, b)$ bzw. $m = lcm(a, b)$.) Mehrere kleinsten gemeinsamen Vielfachen von a und b sind wiederum assoziiert.

91 **Satz: Charakterisierung von Ringen mit** ggT **und** kgV

Sei R ein Integritätsbereich, so sind die folgenden Aussagen äquivalent:

1. $\forall a, b \in R \setminus \{0\}\ \exists s\colon \mathrm{ggT}(a, b) \in R$
2. $\forall a, b \in R \setminus \{0\}\ \exists s\colon \mathrm{kgV}(a, b) \in R$
3. $\forall a, b \in R\colon Ra \cap Rb = R\,\mathrm{kgV}(a, b)$
4. $\forall a, b \in R\colon Ra + Rb = R\,\mathrm{ggT}(a, b)$

Sind diese 4 Bedingungen erfüllt, so gilt außerdem:

$$ab = \mathrm{ggT}(a, b)\,\mathrm{kgV}(a, b)$$

92 **Definition: „Hauptidealring“**
Ein Ring in dem alle Ideale auch Hauptideale sind, heißt Hauptidealring.

93 **Definition: „Primelement“**
Ein Element $p \in R$ heißt Primelement, wenn $p \neq 0$ und $p \notin U(R)$ sowie $\forall a, b \in R: p \mid ab \Rightarrow p \mid a \vee p \mid b$.

94 **Bemerkung: Primideal**
$p \in R \setminus U(R), p \neq 0$ ist genau dann ein Primelement, wenn pR ein Primideal ist.

95 **Definition: „Irredizibilität“**
Ein Element $a \in R \setminus U(R), a \neq 0$ heißt irreduzibel, wenn $a = bc \Rightarrow b \in U(R) \vee c \in U(R)$.

96 **Satz:**
Sei R ein Integritätsbereich, sodass es für alle $a, b \in R$ ein $\mathrm{ggT}(a, b) \in R$ existiert. Dann ist jedes irreduzible Element in R auch ein Primelement. (Das heißt die beiden Begriffe sind dort gleich.)

Beweis (96) Sei $q \in R$ irreduzibel. Wir müssen zeigen, dass q immer prim ist.
Seien nun $a, b \in R$ mit $q \mid ab$ und $d := \mathrm{ggT}(q, a)$. Dann wird q von d geteilt und q ist irreduzibel, also ist entweder $d \sim 1$ oder $d \sim q$.

- 1.Fall: $d \sim 1$
  Dann ist $b = \mathrm{ggT}(qb, ab)$, also wegen $q \mid qb \wedge q \mid ab$: $q \mid b$.
- 2.Fall: $d \sim q$
  Das heißt $\mathrm{ggT}(q, a) = q$ also $q \mid a$.

Beispiel Ein Ring, wo diese Eigenschaft nicht gilt, ist $R = \mathbb{Z}\left[i\sqrt{5}\right] = \left\{ a + ib\sqrt{5} \;\middle|\; a, b \in \mathbb{Z} \right\}$.
Die Abbildung $\varphi: R \to \mathbb{Z}$, $a + ib\sqrt{5} \mapsto a^2 + 5b^2$ ist zwar kein Ringhomomorphismus, jedoch multiplikativ ($\varphi(z_1 z_2) = \varphi(z_1)\varphi(z_2)$). Demnach sind die Einheiten die Elemente z mit $\varphi(z) = 1$ gerade die Einheiten von R: $\{1, -1\}$. In R gilt dann

$$6 = 2 \cdot 3 = \left(1 + i\sqrt{5}\right)\left(1 - i\sqrt{5}\right)$$

Das heißt 3 ist zwar irreduzibel, jedoch nicht prim.

2.4.1 Faktorielle Ringe

97 **Definition: „faktorieller Ring“**
Ein Integritätsbereich R heißt faktorieller Ring, wenn jedes $a \in R \setminus \{0\}$, $a \notin U(R)$ in ein Produkt von Primelementen zerlegt werden kann.

98 **Lemma: Eindeutigkeit von Primfaktorzerlegungen**
Sei R ein Integritätsbereich und $\prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i$ mit Primelementen p_i und irreduziblen Elemente q_i, dann ist bis auf Permutation $p_i \sim q_i$.

Beweis (98) induktiv über n.

99 **Lemma: Projektion von Primfaktorzerlegungen**
Sei R ein Integritätsbereich und $a, b \in R$. Falls ab als Produkt von Primelementen dargestellt werden kann, dann sind sowohl a als auch b bis auf Assoziation in Primelemente zerlegbar.

100 **Satz: Faktoriellitätskriterien**
Sei R ein Integritätsbereich, dann sind folgende Aussagen äquivalent:

1. R ist faktoriell.
2. Alle $a \in R \setminus \{0\} \setminus U(R)$ lassen sich in irreduzible Elemente zerlegen und alle irreduziblen Elemente sind prim.
3. Alle $a \in R \setminus \{0\} \setminus U(R)$ lassen sich in irreduzible Elemente zerlegen und es existiert immer ein größter gemeinsamer Teiler.

Beweis (100) Die Äquivalenz 1. $\Leftrightarrow$ 2. ist trivial (denn in faktoriellen Ringen lassen sich insbesondere die irreduziblen Elemente in Primfaktoren zerlegen). 3. $\Rightarrow$ 1. ist gerade 96. 1. $\Rightarrow$ 3. folgt über die intuitive Konstruktion des ggT aus der Primfaktorzerlegung. □

2.4.2 Euklidische Ringe

101 **Definition: „euklidische Norm, euklidischer Ring“**
Sei R ein Integritätsbereich, dann heißt eine Funktion $\nu\colon R \setminus \{0\} \to \mathbb{N}$ heißt euklidische Norm auf R, wenn es für alle $a, b \in R$, $b \neq 0$ Elemente $q, r \in R$ gibt mit

$$a = bq + r \wedge (r = 0 \vee \nu(r) < \nu(b))$$

Gibt es eine solche euklidische Norm, so nennen wir R einen euklidischen Ring.

Beispiel: die Gaußschen Zahlen In den Gaußschen Zahlen $\mathbb{Z}[i]$ ist das Quadrat der komplexen Norm $\nu\colon \nu(a+ib) := a^2 + b^2$ eine euklidische Norm. Dazu betrachten wir zu $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$ den Quotienten $\frac{\alpha}{\beta}$ in $\mathbb{C}$. Dieser liegt in einem verschobenen Einheitsquadrat der Gaußschen Zahlenebene. Dann wählen wir die Ecke $\gamma \in \mathbb{Z}[i]$ die $\frac{\alpha}{\beta}$ am nächsten liegt und erhalten damit $|\frac{\alpha}{\beta} - \gamma| \leq \frac{1}{\sqrt{2}}$. Also $\nu(\alpha - \beta\gamma) \leq \frac{\nu(\beta)}{2} < \nu(\beta)$ — $\mathbb{Z}[i]$ ist euklidisch.

102 **Satz: Kettenkriterium für faktorielle Ringe**
R ist ein Integritätsbereich. Dann ist R genau dann faktoriell, wenn

1. $\forall a, b \in R \exists c \in R$: $Ra \cap Rb = Rc$ (d.h. es existiert immer ein größter gemeinsamer Teiler) und
2. jede Kette von Hauptidealen in R abbrechen muss: für $a_i \in R$ mit $Ra_i \subseteq Ra_{i+1}$ gibt es ein N sodass $Ra_{n+k} = Ra_n$ für $k \in \mathbb{N}$.

Beweis (102) Die Hinrichtung haben wir für den ersten Punkt bereits in 100 gezeigt. Außerdem bedeutet $Ra_1 \subseteq Ra_i$ gerade $a_i \mid a_1$. Jedoch kann a_1 in einem faktoriellen Ring nur endlich viele Primfaktoren haben und damit sind die a_i für i größer einem gewissen n alle assoziiert.

Für die Rückrichtung genügt es wiederum wegen 100 zu zeigen, dass es eine Zerlegung in irreduzible Faktoren gibt. Wir führen diesen Beweis indirekt:

Angenommen es existiert ein $a \in R$, $a \neq 0$, $a \notin U(R)$ welches sich nicht in irreduzible Elemente zerlegen lässt und sei X die Menge aller solcher Elemente. Dann kann a insbesondere nicht irreduzibel sein: $a = a_1 b_1$, $a_1, b_1 \notin U(R)$, $a_1, b_1 \neq 0$ mit $a_1 \in X$ oBdA. Induktiv erhalten wir somit eine nicht abbrechende, steigende Kette von Hauptidealen mit $Ra_i \subsetneq Ra_{i+1}$ im Widerspruch zur Voraussetzung. Die Annahme ist also falsch, R ist faktoriell. □

103 **Korollar:**
Ein Hauptidealring ist faktoriell.

Beweis (103) Wir zeigen die Behauptung über 102. Punkt 1 ist klar. Ist $Ra_1 \subseteq \cdots \subseteq Ra_n \subseteq \cdots \subseteq R$ eine Kette von Hauptidealen, dann ist $I := \bigcup_{n=1}^{\infty} Ra_n$ ein Ideal in R. Also existiert ein $a \in R$ mit $I = Ra$. □

104 **Satz:**
Sei R ein euklidischer Ring, dann ist R ein Hauptidealring (d.h. insbesondere faktoriell).

Beweis (104) Sei $(0) \neq I \subseteq R$ ein Ideal und $\nu\colon R^* \to \mathbb{N}$ die euklidische Norm. Dann ist

$$N_I := \{\, \nu(a) \mid a \in I \setminus \{0\} \,\} \subseteq \mathbb{N}$$

also gibt es ein $a_0 \in I \setminus \{0\}$ dass N_I nach unten beschränkt. Damit können wir durch a_0 mit Rest teilen:

$$\forall x \in I \exists q, r \in R\colon x = qa_0 + r \qquad r = 0 \vee \nu(r) < \nu(a_0)$$

Dabei ist aber nur $r = 0$ möglich, das heißt $a_0 \mid x$ und somit $Ra_0 = I$.

2.5 Polynomringe

In diesem Abschnitt betrachten wir immer unitäre, kommutative Ringe.

105 **Definition: „Träger“**
Für eine Funktion $f\colon X \to R$ ist der Träger

$$\operatorname{supp}(f) := \{\, x \in X \mid f(x) \neq 0 \,\}$$

Jetzt definieren wir

$$\Gamma(\mathbb{N}, R) := \{\ f: \mathbb{N} \to R \mid |\mathrm{supp}(f)| < \infty\ \}$$

in $\Gamma(\mathbb{N}, R)$ können wir dann kanonisch Addition von Funktionen und Multiplikation mit einem Ringelement definieren. Außerdem definieren wir folgende kommutative Multiplikation:

$$(f \times g)(n) := \sum_{i+j=n} f(i)g(j)$$

Dann ist, wenn wir die Funktionen in Γ als Tupel darstellen:

$$X := (0, 1, 0, \cdots)$$
$$\Rightarrow X^i = \left(\underbrace{0, \cdots, 0}_{i\text{-mal}}, 1, 0 \cdots \right)$$
$$\Rightarrow \left(a_0, a_1, \cdots, a_n, 0, \cdots\right) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

Damit definieren wir:

$$R[X] := \Gamma(\mathbb{N}, R)$$
$$\mathrm{grad}(f) := \max\left\{\ n \in N \;\middle|\; a_n \neq 0\ \right\} \wedge \mathrm{grad}(0) = -\infty$$

und es gilt

$$\mathrm{grad}(fg) \leq grad(f) + grad(g)$$

wobei die Gleichheit nur in Integritätsbereichen allgemein gegeben ist, denn zum Beispiel in $\mathbb{Z}_4$ ist $2 = \mathrm{grad}(\bar{2}X^2) = \mathrm{grad}((\bar{1} + \bar{2}X)(\bar{2}X^2)) < \mathrm{grad}(\bar{1} + \bar{2}X) + \mathrm{grad}(\bar{2}X^2) = 3$.

106 **Definition: „Polynome in mehreren Variablen“**
Die Polynome $R\left[X_1\right]\left[X_2\right]\cdots\left[X_n\right]$ der Form $\mathbb{N} \to (\mathbb{N} \to \cdots R)$ stellen wir dar als Abbildungen $f: \mathbb{N}^n \to R$ und schreiben $R\left[X_1, X_2, \cdots, X_n\right]$.

107 **Bemerkung: Polynomfunktion**
Zu einem Polynom $f \in R[X]$ ist $\bar{f}: R \to R$ die Funktion definiert als

$$\bar{f}(a) := a_0 + a_1 a + \cdots + a_n a^n$$

Dabei ist zu beachten, dass verschiedene Polynome die gleiche Funktion beschreiben können. (z.B. X^p und X in $\mathbb{Z}_p[X]$)

108 **Satz:**
Sei K ein kommutativer Körper, dann ist $K[X]$ ein euklidischer Ring mit grad als Norm.

Beweis (108) Die Division mit Rest in solchen Polynomringen kann mit Polynomdivision durchgeführt werden.