Algebra I

Stand vom 17. November 2014

Dozent: Prof. Dr. Christopher Voll
voll@math.uni-bielefeld.de

Autors: Jonas Betzendahl
jbetzend@techfak.uni-bielefeld.de

Inhaltsverzeichnis

1 Fundamente der Gruppentheorie **3**
1.1 Monoide & Gruppen . . . 3
1.2 Untergruppen und Homomorphismen . . . 4
1.3 Nebenklassen . . . 6
1.4 Normalteiler & Isomorphiesätze . . . 7
1.5 Erzeugungssysteme & zyklische Gruppen . . . 9

2 Fundamente der Ringtheorie **10**
2.1 Ideale, Homomorphismen, Faktorringe . . . 11
2.2 Primfaktorzerlegung . . . 14
2.3 Lokalisierungen, Quotientenkörper, Satz von Gauß . . . 16

3 Übungsaufgaben **19**
3.1 13/10/2014 . . . 19
3.2 15/10/2014 . . . 19

Organisatorisches etc.

Dozent ist Prof. Dr. Christopher Voll
voll@math.uni-bielefeld.de
Büro: UHG V5-238, Sprechstunde noch im Flux

Vorlesungen finden an Montagen von 08.30 Uhr bis 10.00 Uhr und Mittwochs von 14.15 Uhr bis 15.45 Uhr statt.

Es wird darauf hingewiesen, dass die Übungen bei Dr. Doang in Englisch abgehalten werden.

Voraussetzung für die Zulassung zur Prüfung sind das Erreichen von mindestens 50 % der Punkte und mindestens zwei Mal eine aktive Teilnahme an den Übungen (Vorrechnen) abgeleistet zu haben.

Bücher:	Einführung in die Algebra (F. Lorenz, Spektrum)	
	Algebra 1 (S. Bosch, Springer)	
	Algebra (S. Lang, Springer)	
	Algebra (Hungerford)	
	Algebra (v.d. Waerden)	(Ein Klassiker)
	Algebra (E. Artin)	

Übungszettel gibt es immer am Mittwoch der Woche n, bearbeiten werden müssen diese bis Mittwoch der Woche n+1 (Abgabe vor der Vorlesung im Postfach des Tutors), besprochen werden sie in der Woche n+2 in den Tutorien.

Algebra - die Kunst, Gleichungen zu lösen (Einführung)

<u>Lineare</u> Algebra:
$a_{11}x_1 + a_{12}x_2 + \cdots + a_{nm}x_m = b_1$
$\dots$
$a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m = b_n$

Alle Fragen können in Form $a_{ij}, b_i \in \mathcal{K}$ beantwortet werden.
Verallgemeinerung: $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$ (polynom. Gleichung von Grad $n(a_n \neq 0)$.
„Struktur“ der Lösungen solcher Gleichungen treibt Menschen seit Jahrtausenden um.
Spezialfall: Quadratische Gleichungen

$$x^2 + bx + c = 0 \Leftrightarrow \frac{-b \pm \sqrt{b^2 - 4c}}{21}$$

durch Wurzeln lösbar. Kubische Gleichungen:

$$x^3 + bx^2 + cx + d = 0 \Leftrightarrow \dots$$

ebenfalls durch Wurzeln lösbar. Im 16. Jahrhundert wurde bekannt, dass auch quartische Gleichungen ($n = 4$) durch Wurzelausdrücke lösbar sind.
Was nicht ins Weltbild des 16. Jahrhundert passte: Im 19. Jahrhundert zeigte Abel: Nicht jede quintische Gleichung ($n = 5$) kann durch Wurzelausdrücke gelöst werden.
Galois: Lösungen von Polynomen sind nicht einfach Mengen ohne Struktur sondern Mengen **mit** Struktur ($\rightarrow$ Gruppentheorie). Auflösbarkeit von $f = 0$ durch Wurzel $\Rightarrow$ Galois-Gruppe(f) auflösbar.
Ziel der Vorlesung: Einführung in die Sprache der modernen Algebra, sowohl durch Anerkennen der Theorie als auch durch das Praktizieren.

1 Fundamente der Gruppentheorie

1.1 Monoide & Gruppen

Definition 1 *Ein **Monoid** ist eine Menge M zusammen mit einer Verknüpfung $\cdot : M \times M \to M$, die die Eigenschaften erfüllt:*

- `(ASS)` $\forall a, b, c \in M : (a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(Assoziativität)*
- `(NEU)` $\exists\, e = e_M \in M\ \forall a \in M,\ e \cdot a = a = a \cdot e$ *(Existenz eines neutralen Elementes)*

Bemerkung: Die Notation ist oft einfach nur „ab“ statt „$a \cdot b$“, oft auch bei mehreren Monoiden gleichzeitig. Ausgelassen wird immer die passende Verknüpfung. Es wird auch die Schreibweise $\prod_{i=1}^{n} a_i$ für den Ausdruck $a_1 \cdot a_2 \cdot \ldots a_n,\ a_i \in M$ verwendet. Weiterhin gelten per Konvention: $\prod_{i=1}^{n} a_i = e$ für $n \leq 0$ und $a^m = \underbrace{a \cdot a \cdot \ldots a}_{\text{m-mal, } m \in \mathbb{N}}$.

Behauptung: $e \in M$ ist eindeutig (siehe unten).

Sei $a \in M$. Wir nennen $b \in M$ **invers zu** a falls $a \cdot b = b \cdot a = e$ gilt. Falls (!) solch ein b existiert, ist es eindeutig (siehe unten). In diesem Fall ist die Notation oft a^{-1} für b: $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Definition 2 *Eine **Gruppe** ist ein Monoid $(G, \cdot)$ mit der folgenden Eigenschaft:*

`(INV)` $\forall a \in G\ \exists\, a^{-1} \in G$ *sodass* $a \cdot a^{-1} = a^{-1} \cdot a = e$ *(Existenz eines inversen Elements)*

*G heißt **kommutativ** oder synonym dazu **abelsch** falls folgende Eigenschaft gilt:*

`(KOM)` $\forall a, b \in G : a \cdot b = b \cdot a$ *(Kommutativität)*

Vektorräume zum Beispiel sind abelsche Gruppen, die interessante Struktur ist hier aber nicht die abelsche Eigenschaft sondern die Multiplikation mit Skalaren, die sich gut mit der Gruppenstruktur verträgt.

Die **Ordnung** einer Gruppe ist $(G, \cdot)$ ist die Kardinalität $|G|$ von G.

Konvention: „Gruppe G“, falls $\cdot$ klar ist. Ist G abelsch, so schreibt man oft $+$ für $\cdot$ (die Monoidverknüpfung) und man redet von „additiver Schreibweise“ im Gegensatz zu „multiplikativer Schreibweise“. Bei additiver Schreibweise schreibt man oft 0 für e, bzw. bei multiplikativer Schreibweise 1.

Beispiele 1.3:

1. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sind abelsche Gruppen. Ebenso $(\mathcal{K}, +)$ wenn $(\mathcal{K}, +, \cdot)$ ein Körper ist.
2. $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^*, \mathbb{C}^*, \mathcal{K}^* = \mathcal{K} \setminus \{0\}$, mit $1 = e$ als Einselemnent, sind abelsche Gruppen
3. $GL_n(R) = \{x \in Mat_n(R) | \det(x) \neq 0\}$ mit R beliebiger Körper, invertierbare Matrizen über R, $SL_n(R) = \{x \in GL_n(R) | \det x = 1 \in R\}$, ($1_n$ = Einheitsmatrix) sind Gruppen bezüglich der Matrixmultiplikation, mit Einselement jeweils 1_n, allerdings für $n > 1$ <u>nicht</u> abelsch.
4. $\mathbb{N}_0 = \mathbb{N} \cup 0$, $\mathbb{N} = \{1, 2, 3, \ldots\}$. Sowohl $(\mathbb{N}_0, +)$ als auch $(\mathbb{N}, \cdot)$ sind Monoide aber keine Gruppen ($2x = 1$ unlösbar).
5. $Mat_n(R)$ (R Körper) ist ein Monoid ($\cdot$ = Multiplikation, $e = 1_n$).
6. $A \in Mat_n(\mathbb{Z}), L_A = \{x \in {\mathbb{N}_0}^n | xA = 0\}$ ist ein Monoid mit Nullvektor als Einselement.

   Notation: R Ring, dann $R^n = \{(r_1, \ldots, r_n) | r_i \in R\}$ (n-Tupel).
7. Symmetrische Gruppen: Sei X beliebige Menge. $Sym(X) := \{f : X \to X | f \text{ Bijektion }\}$ ist eine Gruppe mit Verknüpfung von Abbildungen als „Multiplikation“. ($f, g \in Sym(X) : f \circ g : X \to X$ Bijektion!), mit $id : X \to X$ als Einselement.

   Rekapitulation der Leibnitz-Formel: K- Körper: $a_{ij} = A \in Mat_n(K)$.

   $$\det(A) = \sum_{\sigma \in S_n} sgn(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}.$$

Wichtiger Spezialfall: $X = \{1, 2, \ldots, n\}, n \in \mathbb{N}$. Setze $S_n = Sym(X)$„ , symmetrische Gruppe vom Grad n“. (Dies erlaubt es, dass jede endliche Gruppe als Unterobjekt verstanden werden kann) Ordnung $|S_n| = n!$. Nicht abelsch falls $n > 2$.

$f \in S_n$:

Matrixschreibweise $\begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$

oder Zykelschreibweise: $(1, f(1), f(f(1)) \ldots)$, $(a, f(a), f^2(a) \ldots)$, $\underbrace{(b, f(b), f^2(b) \ldots)}_{\text{„Zykel“}}$ für $a \notin \{\, f^n(1) \,|\, n = \{1, 2, 3, \ldots\}\,\}$

$\subseteq \{1, \ldots, n\}$ und $b \notin \{\, f^n(1) \,|\, dots\,\} \cup \{\, f^n(a) \,|\, n \in \mathbb{N}\,\}$

Konvention: Zykel der Länge 1 weg.

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \Leftrightarrow (1)(2)(3)$ (A)

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \Leftrightarrow (12)(3)$ (B)

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \Leftrightarrow (123)$ (C)

...

8. Sei X eine beliebige Menge und G eine Gruppe. Dann ist $G^X := Abb(X, G) = \{q : X \to G\}$ mit der folgenden Verknüpfung eine Gruppe:

   Gegeben $\varphi, \psi \in G^X$, definiere für $x \in X$ $\phi \circ \psi := \phi(x) \cdot \psi(x) \in G$ Dies nennt sich „komponentenweise Multiplikation“.

9. Sei X eine beliebige Menge, $\{G_x\}_{x \in X}$, Familie von Gruppen. Dann ist $\prod_{x \in X} G_x = \{\, (g_x)_{x \in X} \,|\, \forall x : g_x \in G_x \,\}$ mit der Verknüpfung $(g_x)_{x \in X} \cdot (h_x)_{x \in X} := (g_x \cdot h_x)_{x \in X}$ – Produkt der Gruppen $G_x, x \in X$.

1.2 Untergruppen und Homomorphismen

Definition 3 *Sei G ein Monoid, $H \subseteqq G$ Teilmenge. H heißt **Untermonoid** von G, falls*

- $e \in H$
- $a, b \in H \Rightarrow ab \in H$

*Ist G eine Gruppe, so heißt H **Untergruppe**, falls zusätzlich*

- $a \in H \Rightarrow a^{-1} \in H$

.

Schreibe gegebenenfalls „$H \leqslant G$“ oder „$H < G$“. Schreibe „$H \lneqq G$“ für Untergruppen $H \neq G$.

Beispiel (1.5):

1. G Gruppe $\Rightarrow H = G \leqslant G$, $\{e\} = G$ heißen **triviale Untergruppen**.
2. $G = (\mathbb{Z}, +), m \in \mathbb{Z}$. $H = m\mathbb{Z} = \{\, mx \,|\, x \in \mathbb{Z}\,\} \leqslant \mathbb{Z}$.
   (a) @1: $0 = m0 \in H$
   (b) @2: $mx(\in H) + my(\in H) = m(x + y) \in H$, $x, y \in \mathbb{Z}$
   (c) @3: Inverses von mx ist $-mx(mx + (-mx) = 0 = e_{\mathbb{Z}})$.

   Tatsache (Beweis später): <u>Jede</u> Untergruppe von Z ist von der Form mZ. $\mathbb{Z} = (-1)Z = 1Z, 0\mathbb{Z} = e_{\mathbb{Z}}$. Schreibe $(m) = m\mathbb{Z}$.

   Echte Untergruppen: $\{A, B\}, \{A, D, E\}, \{A, C\}, \{A, F\}$.
3. G Gruppe, $g \in G$, $H :=< g >:= \{\, g^n \,|\, n \in \mathbb{Z}\,\} \leqslant G$ (!!).

(a)
(b) $g^n \cdot g^m = g^{n+m}$
(c) $(g^n)^{-1} = g^{-n}$

„Die von g erzeugte (zyklische) Untergruppe“ = die kleinste Untergruppe von G, die g enthält (braucht g, g^2, g^3, $\dots$, g^{-1}, $\dots$).

4. $SL_n(K) \leqslant GL_n(K)$, K Körper

   LHS = $\{ x \in Mat_n(K) \,|\, det(x) = 1 \}$ RHS = $\{ x \in Mat_n(K) \,|\, det(x) \neq 0 \}$

   Für alle „vernünftigen“ Körper und alle $n > 1$ ist das eine nicht-triviale Teilmenge.

Definition 4 *(1.6) Seien G, G' Monoide, mit Einselementen $e \in G$ und $e' \in G'$. Ein **Monoidhomomorphismus** ist eine Abbildung $\varphi : G \to G'$, derart, dass*

- $\varphi(e) = e'$
- $\forall a, b \in G : \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

*Sind G, G' Gruppen, spricht man von einem **Gruppenhomomorphismus** (oder oft einfach nur Homomorphismus).*

Bemerkung: Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus, dann gilt
(Übungsaufgaben:)

1. $\forall a \in G : (\varphi(a))^{-1} = \varphi(a^{-1})$. Nach der zweiten Eigenschaft von oben gilt $\varphi(a^{-1}) \cdot \varphi(a) = \varphi(a^{-1} \cdot a) = \varphi(e) = e$
2. $\ker(\varphi) := \{ g \in G \,|\, \varphi(g) = e' \} \leqslant G$.
3. $img(\varphi) = \{ \varphi(g) \,|\, g \in G \} \leqslant G'$

Definition 5 *(1.7) Ein Gruppenhomomorphismus $\varphi : G \to G'$ heißt*

- ***Monomorphismus**, falls er injektiv ist.* ($\Leftrightarrow \ker(\varphi) = \{e\}$),
- ***Epimorphismus**, falls er surjektiv ist.* ($\Leftrightarrow im(\varphi) = G'$),
- ***Isomorphismus**, falls er sowohl ein Epimorphismus als auch ein Monomorphismus ist,*
- ***Endomorphismus** von G, falls $G' = G$,*
- ***Automorphismus** von G, falls $G' = G$ und φ ein Isomorphismus ist.*

Sprechweise: Gegeben ein Isomorphismus heißen G und G' **isomorph zu einander**. Man schreibt $G \cong G'$.
Beispiel: $G = \mathbb{Z}, H = 2\mathbb{Z} \leqslant G$.
Behauptung: $G \to G$, $g \mapsto 2g (= g + g)$ ist Isomorphismus. Also schreibt man $\mathbb{Z} \cong 2\mathbb{Z}$. Isomorphie ist transitiv $(G \cong G'), (G' \cong G'') \Rightarrow G \cong G''$.

Beispiele (1.8):

1. Sei G ein Monoid, $g \in G$, dann ist $\varphi : \mathbb{N}_0 \to G, n \mapsto g^n$ ein Monoidhomomorphismus. (Übungsaufgabe!) φ ist sozusagen bestimmt durch $\varphi(1)$.
2. Ist G sogar eine Gruppe, dann bestimmt $n \mapsto g^n$ einen Gruppenhomomorphismus: $\varphi : \mathbb{Z} \to G$. $im(\varphi) = \{ g^n \,|\, n \in Z \} =< g >$.

   Übungsaufgabe: Wenn $| < g > | = \infty$, dann ist $\phi : \mathbb{Z} \to im(\varphi)$ ein Isomorphismus.
3. Sei G eine Gruppe, $g \in G$. Dann ist $\psi_g := G \to G, h \mapsto ghg^{-1}$ ein Gruppenautomorphismus (Übungsaufgabe: Checken und was ist das Inverse zu ψ_g?).

   $\psi_g(h \cdot h') = ghh'g^{-1} = gheh'g^{-1} = (ghg^{-1})(gh'g^{-1}) = \psi_g(h)\psi_g(h')$. Dies nennt sich „Konjugation mit g“.

   Prüfen: $Aut(G) = \{ \psi : G \to G \,|\, \phi Automorphismus \}$ bildet Gruppe unter Verknüpfung.

   $\{ \phi_g \,|\, g \in G \} < Aut(G) =$ Ïnnere Automorphismen von G”.

1.3 Nebenklassen

Definition 6 *Sei G eine Gruppe, $H \leqslant G$. Eine Menge der folgenden Form: $gH =\{ g \cdot H \mid h \in H \} \subseteq G, g \in G$ heißt **Linksnebenklasse** (LNK) (left coset) von H in G.*
Dementsprechend: $Hg = \{ h \cdot g \mid h \in H \}$ heißt Rechtsnebenklasse (RNK) von H in G.

Nebenklassen „pflastern“ die Gruppe.
Lemma (1.10): Seien gH und $g'H$, mit $g, g' \in H$ Linksnebenklassen von $H \leqslant G$. Dann sind Äquivalent:

1. $gH = g'H$
2. $gH \cap g'H \neq \varnothing$
3. $g \in g'H$
4. $g'^{-1}g \in H$

Beweis:

1. klar: $gH \ni ge = g \Rightarrow gH \neq \varnothing$
2. $gh \in g'H$ für ein $h \in H$. $\Rightarrow \exists h' \in H : gh = g'h' \Leftrightarrow g \underbrace{hh^{-1}}_{e} = g' \underbrace{h'h^{-1}}_{\in H} \Leftrightarrow g \in g'H$.
3. $g \in g'H \Leftrightarrow \exists h \in H : g = g'h \Rightarrow (g')^{-1} \cdot g = h \in H$.
4. $(g')^{-1}g \in H$, etwa $(g')^{-1}g = h \in H \Rightarrow g = g' \cdot h$. $gH =\{ g\tilde{h} \mid \tilde{h} \in H \} = \{ g' \cdot (h\tilde{h}) \mid \tilde{h} \} = g'H$ □

Satz (1.11): Je zwei Linksnebenklassen von H in G sind in Bijektion zueinander. Verschiedene LNK sind disjunkt. Insbesondere ist G disjunkte Vereiningung der Linksnebenklassen von H in G. **Beweis:** @Bijektion: Gegeben gH, $g'H$, $g, g' \in G$.
$gH \underbrace{\cong}_{(bijektiv)} H$. $(gH \cong eH = H \cong g'H)$
Es reicht zu zeigen: $H \to gH, h \mapsto gh$ ist Bijektiv. $gh = gh' \leftrightarrow g^{-1}gh = g^{-1}gh' \leftrightarrow h = h'$. □

Definition 7 *(1.12) Sei G eine Gruppe, $H \leqslant G$. Schreibe $G/H = \{ gH \mid g \in G \}$ für die Menge der Linksnebenklassen von H in G und $H \setminus G = \{ Hg \mid g \in H \}$ für die Menge der Rechtsnebenklassen von H in G.*

Bemerkung: $G/H \to H \setminus G, gH \mapsto Hg$ ist Bijektion.
ÜA: $(gH = g'H \Leftrightarrow g \cdot (g')^{-1} \in H \Leftrightarrow Hg = Hg')$

Definition 8 *(1.13) Setze $|G : H|(= [G : H] = (G : H)) = |G/A| = = |H \setminus G|$ genannt der **Index** von H in G.*

Informell: $|G : H|$ „inverse Dichte“ von H in G. $\frac{1}{|G:H|}$ =„$P(g \in H)$“.
z.B.: $G = \mathbb{Z}, H = m\mathbb{Z}. \to |G : H| = m$.
Beispiel (1.14) :

1. $H = \{e\} : G/H \cong H \setminus G \cong G \Rightarrow |G : H| = |G|$.
2. $H = G : G/G = G$
   $G = \{\cdot\} \Rightarrow |G : G| = 1$.
3. Drittes Beispiel siehe oben.

Korrollar (1.5) (Satz von Lagrange): Sei G eine <u>endliche</u> Gruppe, $H \leqslant$. Dann gilt $|G| = |H| \cdot |G : H|$. $(\frac{|G|}{|H|} = |G : H|)$.
(1.16) Insbesondere teilt $|H|$ stets $|G|$!
Achtung: $\exists$ endliche Gruppen G mit der Eigenschaft, dass einige Teiler ihrer Ordnung von von Untergruppen H realisiert werden. (ÜA: Eleganter formulieren.)
z.B: Ist p eine Primzahl, $|G| = p^e, e \in \mathbb{N}_0$, so heißt G **p-Gruppe.** Aus Langrange folgt: $\forall H \leqslant G, H$ ist p-Gruppe.

1.4 Normalteiler & Isomorphiesätze

Definition 9 *(1.17) Sei G eine Gruppe, $H \leqslant G$ heißt **Normalteiler** (oder synonym dazu: normale Untergruppe), wenn $\forall g \in G\ gH = Hg$. Gegebenenfalls heißt gH die von g bestimmte Nebenklasse von H in G. Gegebenenfalls schreibe $(H \trianglelefteq G) \Leftrightarrow H \triangleleft G$.*

Bemerkung: g, H, G wie in (1.17): $gH = Hg \Leftrightarrow gHg^{-1} = H$.
Um zu verifizieren, ob $H \leqslant G$ ein Normalteiler ist, reicht es zu testen, ob $\forall g.gHg^{-1} \subseteq H$ (*).
In der Tat. Angenommen (*) gilt, so gilt auch $\forall g \in G.gH \subseteq Hg$. Aber es gilt $g^{-1}Hg^{-1^{-1}} = g^{-1}Hg \subseteq H$, d.h. $Hg \subseteq gH$
$\Rightarrow gH = Hg$
Beispiel (1.18):

1. $\{e\} \triangleleft G$. $(\forall g : g\{e\} = \{e\}g = \{g \cdot e\} = \{g\})$. Ebenso: $G \triangleleft G : gG = G = Gg$.

2. Ist G abelsch, ist <u>jede</u> Untergruppe Normalteiler.

3. $G = S_3$. Die Untergruppen H von S_3 die von $\{e\}$ und S_3 selbst verschieden sind, sind $\{< (12) >, < (13) >, < (23) >, < (123) >\}$ (Untergruppen der Ordnung 2,2,2 und 3. Lagrange sagt dass es keine anderen geben kann.) Übungsaufgabe: Von diesen 4 Untergruppen ist nur $< (123) >$ normal.

4. Ist $\varphi : G \to G'$ Gruppenhomomorphismus, dann ist $ker(\varphi) = \{g \in G | \varphi(g) = e_{G'}\} \triangleleft G$.
   Z.z. $\forall g \in G.g(ker\varphi)g^{-1} \subseteq ker\varphi$. Sei gkg^{-1} mit $k \in ker\varphi$. Reicht zu zeigen: $\varphi(gkg^{-1}) = e_{G'}$. Aber

$$\begin{aligned} \varphi(gkg^{-1} &= \varphi(g)\varphi(h)\underbrace{\varphi(g^{-1})}_{=\varphi(g)^{-1}} \\ &= \varphi(g)e_{G'}\varphi(g)^{-1} \\ &= \varphi(g)\varphi(g)^{-1} = e_{G'} \end{aligned}$$

Sei $N \triangleleft G$. Wollen Gruppenstruktur auf $G/N = \{gN | g \in G\}$.
Allgemein $X, Y \subseteq G : XY := \{xy | x \in X, y \in Y\} \subseteq G$
Definiere $\cdot : G/N \times G/N \to G/N, (gN, kN) \mapsto ghN$
$gN = g'N \Leftrightarrow g(g')^{-1} \in N$

Seien also $g' \in G, k' \in G$ mit $gN = g'N, kN = k'N$. Wir wissen, $g(g')^{-1} =: n_1 \in N, k(k')^{-1} =: n_2 \in N$.
Zu zeigen: $gkN = g'k'N$, d.h. $gh(g'h')^{-1} \in N$. Nun ist

$$\begin{aligned} gh(g'h')^{-1} &= g\underbrace{h(h')^{-1}}_{n_2}(g')^{-1} \\ &= gn_2(g')^{-1} \\ &= gn_2g^{-1}\underbrace{g(g')^{-1}}_{n_1} \\ &= \underbrace{gn_2g^{-1}}_{\in N, da N \triangleleft G}\ n_1 \in N \end{aligned}$$

Übungsaufgabe: Verifiziere, dass $\cdot$ eine Gruppenoperation ist.
Bemerkung: $N \triangleleft G$. Die Gruppe G/N („G modulo N“) heißt „Faktorengruppe von G nach N“.
$\pi : G \to G/N, g \mapsto gN$ heißt die „natürliche Reduktion“, „natürlicher Homomorphismus“, „natürliche Surjektion“, „Reduktionmodulo N“.
π ist Epimorphismus. $(g, k \in G : \underbrace{\pi(gh)}_{ghN} = \underbrace{\pi(g)\pi(h)}_{gN \cdot hN})$

Satz 1 (1.19) *„Homomorphiesatz“ Sei $\varphi : G \to G'$ Homomorphismus von Gruppen G, G' und sei $N \triangleleft G$ mit $N \leq ker\varphi$. Dann existiert **genau ein** Homomorphismus $\bar{\varphi} : G/N \to G'$, derart, dass $\varphi = \bar{\varphi} \circ \pi$.*

$$\begin{tikzcd} & G \arrow[dl, "\pi"] \arrow[d, "\varphi"] \\ G/N \arrow[r, leftrightarrow, "\bar{\varphi}"] & G' \end{tikzcd}$$

Es gilt:

- $im(\bar{\varphi}) = im(\varphi)$
- $ker(\bar{\varphi}) = \pi(ker(\varphi)) \lhd G/N$
- $ker(\varphi) = \pi^{-1}(ker(\bar{\varphi})) \lhd G$

Beweis: Eindeutigkeit. Angenommen $\bar{\varphi}$ mit $\varphi = \bar{\varphi} \circ \pi$ existiert $\forall g \in G.\bar{\varphi}(gN) = \bar{\varphi}(\pi(g)) = \varphi(g)\Box$
Existenz: Gegeben $gN \in G/N$. Definiere $\bar{\varphi}(gN) := \varphi(g)$. Wohldefiniert?
In der Tat, seien $g, g' \in G : gN = g'N$, das heißt $g = g'n \exists n \in N$. Zu zeigen: $\varphi(g = \varphi(g')$.
$\varphi(g) = \varphi(g'n) = \varphi(g')\varphi(n) = \varphi(g')$, da $N \leq her\varphi$.
Homomorphieeigenschaft: Seien $gN, hN \in G/N$.
$\bar{\varphi}(gN \cdot hN) = \bar{\varphi}(ghN) = \varphi(gh) = \varphi(g)\varphi(h) = \bar{\varphi}(gN) \cdot \bar{\varphi}(hN)$

1. $ker\varphi = \pi^{-1}(ker(\bar{\varphi})$, da $\varphi = \bar{\varphi} \circ \pi$
2. $im(\bar{\varphi}) = im(\varphi), ker\bar{\varphi} = \pi(ker\varphi)$, da π **surjektiv** ist.$\Box$

Beachte: $\bar{\varphi}$ Monomorphismus gdw. $ker\bar{\varphi} = N$ gdw. $ker\varphi = N$
Nenne $\bar{\varphi}$ den von φ auf G/N **induzierten** Homomorphismus.

Korrolar 1 (1.20) *Ist φ ein Epimorphismus, dann gilt $G/ker(\varphi) \to G'$ ist Isomorphismus von Gruppen.*

Satz 2 (1.21) *1. Isomorphiesatz Sei G Gruppe, $H \leq G$, $N \lhd G$.*

- *$HN \leq G$ ist Untergruppe (nicht nur Teilmenge). $N \lhd HN$*
- *$H \cap N \lhd H$*
- *$\varphi : H/H \cap N \to HN/N, h(H \cap N) \mapsto hN$ ist Isomorphismus*

Beweis:
Übungsaufgabe: G Gruppe, $X \subseteq G$: $X \leq G$ gdw. 1. $X \neq \emptyset$, 2. $\forall x, y \in X : x(y)^{-1} \in X$
@1: $HN \ni e \cdot e = e, \Rightarrow HN \neq \emptyset$
$h_1n_1, h_2n_2 \in HN, h_i \in H, n_i \in N$

Zu zeigen: $h_1n_1(h_1n_1)^{-1} \in HN$. In der Tat $h_1n_1n_2^{-1}h_2^{-1} = \underbrace{h_1h_2^{-1}}_{\in H}\overbrace{(h_2 \underbrace{n1n_2^{-1}}_{\in N} h_2^{-1})}^{\in N, da N \lhd G} \in HN$

$N \leq HN, N \lhd G$ impliziert, dass $N \lhd HN$:
$N \lhd G \Leftrightarrow \forall g \in G : gNg^{-1} \subseteq N \Rightarrow \forall k \in HN : kNk^{-1} \subseteq N \Leftrightarrow N \trianglelefteq HN$
Bemerkung: $(HN)/N nicht \cong H$. Z.B. $HH/H = H/H = \{e\}$
Betrachte $\psi : H \to HN/N, h \mapsto heN = hN$ offensichtlich Epimorphismus.
$ker\psi = \{h \in H | kN = N\} = H \cap N$ (@2)

Korrolar 2 (1.22) *$H/(H \cap N) \to HN/N$ ist Isomorphismus* $\Box$

$$\begin{array}{c} G \\ \downarrow{\scriptstyle G/H} \\ H\,{\scriptstyle G/N} \\ \downarrow{\scriptstyle H/N} \\ N \end{array}$$

Satz 3 (1.22) *2. Isomorphiesatz Sei G eine Gruppe, $N, H \trianglelefteq G, n \leq H$. Dann auch $N \trianglelefteq H, H/N \trianglelefteq G/N$ und $G/N/H/N \simeq G/H$.*

Beweis: Betrachte $\psi : H \hookrightarrow G \xrightarrow{\pi_n} G/N, h \mapsto k \mapsto kN$, Homomorphismus. $\ker \psi = N$, insbesondere $N \trianglelefteq H$.
Aus dem Homomorphiesatz folgt, dass dies ein Monomorphismus ist. $H/N \to G/N$, konkret: $H/N =\{\, hN \,|\, h \in H \,\}$ $\subseteq G/N = \{\, gN \,|\, g \in G \,\}$. Identifiziere H/N mit Untergruppe von G/N!
Beachte: $H = \ker_{\pi_H}$, $\pi_H : G \to G/H, g \mapsto gH$. $N \leq \ker \pi_H$. Aus dem Homomorphiesatz folgt, dass dies ein Epimorphismus ist. $G/N \to G/H, gN \mapsto gH$ mit Kern H/N.
Nach Korollar 1.20: $G/N/H/N \simeq G/H\Box$.

1.5 Erzeugungssysteme & zyklische Gruppen

Definition 10 *(1.23) Sei G eine Gruppe und $X \subseteq G$.*

$$\langle X \rangle \coloneqq \bigcap_{X \subseteq H \leqslant G} H \leqslant G$$

*heißt dann die **von** X **erzeugte** Untergruppe, die kleinste Untergruppe von G, die X enthält.*
***Spezialfall:** $\langle X \rangle = G$. Nenne X ein **Erzeugendensystem** (generating set / system) von G.*
*Setze $d(G) \coloneqq min\{\, |Y| \,|\, Y \text{ EZS von } G\} \in \mathbb{N} \cup \{\infty\}$. G heißt **zyklisch** falls $d(G) = 1$. $d(G)$ heißt **(minimale) Erzeugerzahl** von G.*

Übungsaufgabe: $d(S_n) = ?$
Bemerkungen:

1. $X \leqslant G, \langle X \rangle = X$.
2. $\langle X \rangle = \{\, x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_m^{\varepsilon_m} \,|\, m \in \mathbb{N}_0, x_i \in X, \varepsilon_i \in \{-1, 1\} \,\}$
   $(x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m})^{-1} = (x_m^{\varepsilon_m} x_{m-1}^{\varepsilon_{m-1}} \dots x_1^{\varepsilon_1})$
3. Für $g \in G \quad < g > = \{\, g^n \,|\, n \in \mathbb{Z} \,\} = \langle \{g\} \rangle$. (Notation von letzter Woche)
4. G zyklisch $\Leftrightarrow \exists g \in G : G = < g > \Leftrightarrow \exists$ Epimorphismus: $\varphi : \mathbb{Z} \to G, 1 \mapsto g$.

Beispiel: (1.24)

1. $(\mathbb{Z}, +)$ zyklisch $(\varphi = \mathtt{id}_{\mathbb{Z}})$.
2. Für $m \in \mathbb{Z} : \mathbb{Z}/(m) = \mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \dots, m - 1 + m\mathbb{Z}\}$
   (Nebenklassen von $m\mathbb{Z} \trianglelefteq \mathbb{Z}$!)
   Epimorphismus: $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, u \mapsto r(u) + m\mathbb{Z}$
   Division mit Rest: $\exists a, r \in \mathbb{Z}. u = a \cdot m + r, 0 \leqslant r \leqslant m - 1$
   Lemma (1.25): Sei $H \leqslant \mathbb{Z}$. Dann existiert $m \in \mathbb{N}_0$. $H = m\mathbb{Z}$.

Beweis: Wenn $H = \{0\}$, dann $H = 0 \cdot \mathbb{Z}$. OBdA sei $H \neq \{0\}$.
Sei $m \in H \setminus \{0\}$ das kleinste positive Element von H. Behauptung: $H = m\mathbb{Z}$ „$\supseteq$“klar, da $H \leqslant \mathbb{Z}$. Sei $h \in H. \exists b, r \in \mathbb{Z} : h = b \cdot m + r, 0 \leq r < m \Rightarrow h - bm = r \in H$. Nach Wahl von m ist $r = 0 \Rightarrow \perp$. $\square$

Satz 4 (1.26) *Sei G eine zyklische Gruppe, dann gilt:*

$$G \simeq \begin{cases} \mathbb{Z}\,(= \mathbb{Z}/(0))\,, & \text{falls } |G| = \infty \\ \mathbb{Z}/m\mathbb{Z}, & \text{falls } |G| = m < \infty \end{cases}$$

Beweis: Sei $G = \langle g \rangle, g \in G$. Dann ist $\varphi : \mathbb{Z} \to G, n \mapsto g^n$ ist ein Epimorphismus. Nach Korrolar 1.20 ist $\mathbb{Z}/(\ker\varphi) \simeq G$. Aus Lemma 1.25 folgt $\ker\varphi = m\mathbb{Z}, m \in \mathbb{N}_0$.
$m = 0 \Rightarrow G \simeq \mathbb{Z}$. $m > 0 : G \simeq \mathbb{Z}/(m\mathbb{Z}), |G| = m$. $\square$

Satz 5 (1.27) *Sei G zyklisch. (1) Jede Untergruppe von G ist zyklisch. (2) Ist $\varphi G \to G'$ (G' beliebige Gruppe!) ein Homomorphismus, dann sind $\ker\varphi$ und $Im\varphi$ zyklisch*

Beweis: @2: „$\ker\varphi \leqslant G$ zyklisch“ folgt aus (1). $G = \langle g \rangle, g \in G$. $\mathrm{Im}\varphi = \{\, \varphi(h) \,|\, h \in G \,\} = \{\, \varphi(g^n) \,|\, n \in \mathbb{Z} \,\} = \{\, \varphi(g)^n \,|\, n \in \mathbb{Z} \,\} = \langle \varphi(g) \rangle \leqslant G'$.
@1: Sei $H \leq G$. Sei $\psi : \mathbb{Z} \to G$ ein Epimorphismus. Betrachte $\underbrace{\psi^{-1}(H)}_{=K} \leqslant \mathbb{Z}$ - zyklisch! Insbesondere ist $\psi(K) = H$ - zyklisch nach (2).

Definition 11 *Sei G eine Gruppe, $g \in G$. Ordnung von $g \coloneqq |\, \langle g \rangle \,|$, geschrieben $|g|$.*

Satz 6 (1.29) *(Kleiner Satz von Fermat) Sei G eine endliche Gruppe, $g \in G$. Dann teilt $|g|$ die Ordnung $|G|$ und es gilt $g^{|G|} = e$.*

Beweis: Betrachte den Epimorphismus $\varphi : \mathbb{Z} \to \langle g \rangle = H \leqslant G$, mit $\ker\varphi = m\mathbb{Z}, m \in \mathbb{N}$.
$|G| < \infty \Rightarrow |H| = |\, \langle g \rangle \,| = |g|$ teilt $|G|$. $H \simeq \mathbb{Z}/m\mathbb{Z} \Rightarrow |H| = m = |g|$.
$(g^m)^{|G|/m} = e^{|G|/m} = e\square$

2 Fundamente der Ringtheorie

Bis aif weiteres: R kommutativ.

Definition 12 *(2.1) Ein **Ring** (mit Einselement 1) ist eine Menge R mit $+ : R \times R \to R, (x,y) \mapsto x+y$, $\cdot : R \times R \to R, (x,y) \mapsto x+y$, derart, dass*

1. *$(R,+)$ abelsche Gruppe (in äddítiver Notationmit Neutralelement $0 \in R$)*
2. *$(R,\cdot)$ Monoid*
3. *Distributivgesetze gelten: $\forall a,b,c \in R : (a+b)\cdot c = a\cdot c + b\cdot c, c\cdot(a+b) = c\cdot a + c\cdot b$.*

*R heißt **kommutativ**, falls $\forall a,b \in R : ab = ba$.*

Definition 13 *(2.2) Ein **Unterring** eines Ringes $(R,+,\cdot)$ ist eine Teilmenge S, die bezüglich $+$ und $\cdot$ ein Ring ist. S sei eine additive Untergruppe von $(R,+)$ und ein Untermonoid von $(R,\cdot)$.*
*Das Paar $S \subset R$ heißt auch **Ringerweiterung**.*

Definition 14 *(2.3) Sei R ein Ring. $R^* = \{ a \in R \,|\, \exists b \in R \}$: $ab = ba = 1$ - Einheitengruppe („unit group“) von R. $a \in R$ heißt **Einheit**, falls $a \in R^*$.*

- *R heißt Schiefkörper („skew field“) falls $R \neq \{0\} und R^* = R \setminus \{0\}$, d.h. jedes von 0 verschiedenes Element in R ist invertierbar.*
- *Ein **Körper** („field“) ist ein Schiefkörper, bei dem Multiplikation kommutativ ist: $\forall a,b \in R : ab = ba$.*
- *Ein Element $a \in R$ heißt **Nullteiler** („zeri divisor“) falls $\exists b \in R \setminus \{0\} : ab = 0$ oder $ba = 0$. ($0 \in R$ ist Nullteiler!)*
- *R heißt **nullteilerfrei**, **Integritätsbereich**, **Integritätsring** („(integral) domain“) falls $R \neq \{0\}$ und $R \setminus \{0\}$ keine Nullteiler hat.*

Übungsaufgabe: $(R*, \cdot)$ ist Gruppe!
Bemerkung: `Warnung`: $a,b,c \in R, ac = bc \leftrightarrow ac - bc = (a-b)c = 0$. Wenn R Integritätsbereich ist und $c \neq 0$), folgt hierais $a = b$.

Beispiel: (2.4):

1. $(\mathbb{Z},+,\cdot)$ ist ein Ring. $\mathbb{Z}^* = \{1,-1\}$, Nullteiler: $\{0\} \Rightarrow \mathbb{Z}$ ist Integritätsbereich!
2. R kommutativ. Dann ist $\mathrm{Mat}_n(R)$ ist Ring mit $1 = E_n$ und der Nullmatrix als Nullelement.

   $\mathrm{Mat}_n(R)^* = \{ A \in Mat_n(R) \,|\, \exists B \in Mat_n(R) : AB = BA = E_n \} = \{ A \in Mat_n(R) \,|\, detA \underline{\in R^*} \} = GL_n(R)(= GL(n;R))$. (general linear)

   Zum Beispiel: $GL_n(\mathbb{Z}) = \{ A \in Mat_n(\mathbb{Z}) \,|\, detA \in \{-1,1\} \}$

   $n > 1 : Mat_n(R)$ im Allgemeinen kein Integritätsbereich: $\exists A : A^m (= A \cdot A^{m-1}) = 0$ für geeignetes m.
3. Hamiltonische Quaternionen

   $\mathbb{H} = \langle e,i,j,k \rangle_{\mathbb{R}} = \mathbb{R}e \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k = \{ a_1 e + a_2 i + a_3 j + a_4 k \,|\, a_i \in \mathbb{R} \}$

   Multiplikationstabelle:

·	e	i	j	k
e	e	i	j	k
i	i	-e	k	-j
j	j	-k	-e	i
k	k	j	-i	-e

   $(a_1 e + a_2 i + a_3 j + a_4 k)(b_1 e + b_2 i + b_3 j + b_4 k) = a_1 b_1 \underbrace{e \cdot e}_{e} + a_1 b_1 \underbrace{e \cdot i}_{i} + \dots + a_3 b_4 \underbrace{j \cdot k}_{i} + \dots$

   Tatsache / Übungsaufgabe: $(\mathbb{H},+,\cdot)$ ist ein Schiefkörper aber kein Körper.

   $\mathbb{H} = \underbrace{\underbrace{\mathbb{R}e}_{\simeq\mathbb{R}} \oplus \mathbb{R}i}_{\simeq\mathbb{C}} \oplus \mathbb{R}j \oplus \mathbb{R}k$

$$\begin{array}{c}
\mathbb{H} \simeq_{\mathbb{R}} \mathbb{R}^4 \\
\Big| \\
\mathbb{C} \simeq_{\mathbb{R}} \mathbb{R}^2 \\
\Big| \\
\mathbb{R}
\end{array}$$

Von $\mathbb{R}$ zu $\mathbb{C}$ wird etwas gewonnen (algebraische Abgeschlossenheit, von $\mathbb{C}$ zu $\mathbb{H}$ wird allerdings etwas sehr wichtiges verloren (Kommutativität der Multiplikation). Diese Reihe könnte noch weiter gehen, dann wird es aber irgendwann uninteressant.

4. Sei X eine Menge, $X \neq \varnothing$, $(R_x)_{x\in X}$ eine Familie von Ringen, dann ist $P = \prod_{x\in X} R_x$ ein Ring mit Addition $(r_x) + (s_x) = (r_x + s_x)_x$ und der Multiplikation $(r_x)(s_x) = (r_x \cdot s_x)_x$.

   Null: $(0_x)_x$, Eins: $(1_x)_x$

   Achtung: P hat Nullteiler, auch wenn alle R_x nullteilerfrei sind: $|X| = 2 : P = \mathbb{Z} \times \mathbb{Z} = \prod_{x\in X} \mathbb{Z}, a = (1,0), b = (0,1) \Rightarrow a \cdot b = (0,0)$

Definition 15 *(2.5) (Polynomring in einer Variablen) Sei R ein kommutativer Ring. Der* ***Ring der Polynume in einer Variablen*** *X (Polynomring) mit* ***Koeffizienten in*** *R ist*
$R[X] = \mathbb{R}^{\mathbb{N}_0} = \{ (a_0, a_1, \dots) \mid \forall i \in \mathbb{N}_0 : a_i \in \mathbb{R}. Für\ fast\ alle\ i : a_i = 0 \}$ mit Addition $(a_i)_{i\in\mathbb{N}_0} + (b_i)_{i\in\mathbb{N}_0} = (a_i + b_i)_{i\in\mathbb{N}_{\not 0}} (\in R[x])$.
Multiplikation: $(a_i)_{i\in\mathbb{N}_0} \cdot (b_i)_{i\in\mathbb{N}_0} = (c_i)_{i\in\mathbb{N}_0} \in R[X]$ wobei für $i \in \mathbb{N}_0 : c_i \coloneqq \sum_{r+s=i} a_r b_s) = \sum_{j=0}^{i} a_j b_{i-j}$
Schreibe $f(X) = \sum_{i=0}^{\infty} a_i X^i = \sum_{i=0}^{N} a_i X^i (n >> 0 : a_i = 0$ falls $i \geq N)$ anstelle von $(a_i)_{i\in\mathbb{N}_0} \in R[X], g(X) = \sum_{i=0}^{\infty} b_i X^i$
$f(X) \cdot g(X) = \sum_{i=0}^{\infty} c_i X^i$
Idee: *$R \subset S$ Ringerweiterung, $f(X) \in R[X] :\rightsquigarrow f : S \to S, s \mapsto f(s) = \sum_{i=0}^{\infty} a_i s^i \in S$, die von f induzierte„polynomielle Funktion“.*
$R = \mathbb{F}_2 = \{0,1\} : f(X) =)X^2 - X = (0,-1,1,0,\dots), g(X) = 0 = (0,0,\dots), \quad \mathbb{F}_2 \to \mathbb{F}_2, s \mapsto s^2 - s = 0$!
Polynome sind verschieden von Polynomfunktionen!

Definition 16 *(2.6) Sei $f = (a_i)_{i\in\mathbb{N}_0} \in R[X], R$ ein kommutativer Ring. Für $i \in \mathbb{N}_0$ ist a_i der i-te Koeffizient von f. Der* ***Grad*** *(„degree“) von $f(\neq 0)$ ist $\max \{ i \mid a_i \neq 0 \}$, geschrieben $\deg(f)$. $\deg(0) = -\infty$.*
Sei $f \neq 0$. Dann ist der Leitkoeffizient von $f = a_{\deg f}$. Ist $a_{\deg f} = 1$, so heißt f ***normiert.***

Satz 7 (2.7) *(Polynomdivision mit Rest) Sei R ein kommutativer Ring, $g = (a_i) \in R[X]$, dessen Koeffizient $a_{\deg(g)}$ eine Einheit in R ist. Dann gibt es zu jedem $f \in R[X]$ eindeutig bestimmte $q, r \in R[X] : f = q \cdot g + r, \deg(r) < deg(g)$.*

2.1 Ideale, Homomorphismen, Faktorringe

Definition 17 *(2.8) Sei R ein Ring. Eine Teilmenge $I \subseteq R$ heißt* ***Ideal (von*** *R***)*** *falls gilt:*

1. $0 \in I$
2. $\forall a, b \in I : a + b \in I$
3. $\forall a \in I, b \in R : ab \in I$

Äquivalent: I additive Untergruppe von R, abgeschlossen bezüglich Multiplikation mit Elementen von R. Gegebenenfalls schreibe $I \trianglelefteq R$

Sind $I_1, I_2 \trianglelefteq R$, so sind:
$I_1 + I_2 = \{ i_1 + i_2 \mid i_1 \in I_1, i_2 \in I_2 \} \trianglelefteq R$.
$I_1 \cdot I_2 = \{ \sum_{\text{endlich}} i_1 i_2 \mid i_1 \in I_1, i_2 \in I_2 \} \trianglelefteq R$.
$I_1 \cap I_2 = \{ i \in R \mid i \in I_1 \text{ und } i \in I_2 \} \trianglelefteq R$.
Allgemeiner: Gegeben eine Familie $(I_x)_{x\in X}$ von Idealen von R (d.h. $I_x \trianglelefteq R \forall x \in X$), definiere
$\sum_{x\in X} I_x \coloneqq \{ \sum_{x\in X} i_x \mid \forall x \in X : i_x \in I_x; i_x = 0 \text{ für fast alle } x \in X \}$.
Für $i \in I$ schreibe:
$(i) \coloneqq \{ ib \mid b \in R \} =: iR \trianglelefteq$, das von i erzeugte **Hauptideal** (principal ideal).
Check:

1. $0 = i \cdot 0 \in (i)$
2. $ib_1 + ib_2 = i(b_1 + b_2) \in (i)$ für $b_i \in R$
3. $(ib)b' = i(bb') \in (i)$ für $b, b' \in R$

Definition 18 *(2.9)*

1. *Sei R ein Ring und X eine Menge. Sei $(i_x)_{x \in X}$ eine Familie von Ringelementen. Dann heißt $I = \sum_{x \in X}(i_x) \trianglelefteq R$ das von den i_x* ***erzeugt Ideal****. Das kleinste Ideal, das die Elemente i_x enthält. Die Familie $(i_x)_{x \in X}$ heißt (ein)* ***Erzeugendensystem****.*
2. *$I \trianglelefteq R$ heißt* ***endlich erzeugt****, falls es ein endliches Erzeugendensystem zulässt.*
3. *$I \trianglelefteq R$ heißt* ***Hauptideal****, falls es ein Erzeugendensystem der Kardinalität 1 zulässt. $\exists i \in R : I = (i)$.*
4. *Ist R ein Integritätsbereich, und ist jedes Ideal von R ein Hauptideal, dann heißt R ein* ***Hauptidealring*** *(principal ideal domain).*

Proposition (2.10): $(\mathbb{Z}, +, \cdot)$ ist ein Hauptidealring.
Beweis: $\mathbb{Z}$ ist offensichtlich Integritätsbereich. Ideale in $\mathbb{Z}$ sind insbesondere additive Untergruppen. Die Untergruppen von $\mathbb{Z}$ sind alle von der Form $m\mathbb{Z} = (m) = \{\, m \cdot n \,|\, n \in \mathbb{Z} \,\}, m \in \mathbb{N}_0$ $\square$

Beispiel (2.11):

1. Der Ring $\mathbb{Z}[X]$ ist kein Hauptidealring: z.B. $I = (2, X) \trianglelefteq \mathbb{Z}[X]$ (Gegeben Elemente $i_1, \ldots, i_n \in R : (i_1, \ldots, i_n) \coloneqq \sum_{j=1}^{n}(i_j) \trianglelefteq R$)

   $(2) \trianglelefteq \mathbb{Z}[X] : (2) = \{\, 2 \cdot f \,|\, f \in \mathbb{Z}[X] \,\} = \{\, \sum_{i=0}^{\infty} a_i x^i \,|\, \text{fast alle } a_i = 0, a_i \in (2) \leqslant \mathbb{Z} \,\}$

   $(X) = \{\, X \cdot f \,|\, f \in \mathbb{Z}[X] \,\} = \{\, \sum_{i=0}^{\infty} a_i x^i \,|\, \text{fast alle } a_i = 0, a_0 = 0 \,\}$

   $(2, X) = (2) + (X) = \{\, f \in \mathbb{Z}[X] \,|\, f = \sum_{i=0}^{\infty} a_i x^i, \text{fast alle } a_i = 0, a_0 = 0 \,\}$

   Behauptung: $(2, X)$ ist kein Hauptideal (ÜA!)
2. Ist R ein Körper, so gibt es **nur** die Ideale $(0) = \{0\}$ und $(1) = \{\, 1 \cdot r \,|\, r \in R \,\} = R$. Sei etwa $x \in I \setminus \{0\}$. Dann ist $x \cdot x^{-1} = 1 \in I$, das heißt $I = (1) = R$.

Definition 19 *(2.12) Seien R, R' Ringe. Eine Abbildung $\varphi : R \to R'$ heißt* ***Ringhomomorphismus****, falls*

1. *$\forall a, b \in R : \varphi(a + b) = \varphi(a) + \varphi(b)$*
2. *$\varphi(1) = 1, \forall a, b \in R : \varphi(ab) = \varphi(a)\varphi(b)$.*

(d.h. φ sei Homomorphismus abelscher Gruppen und Monoiden).
Die in Definition 1.7 eingeführten Begriffe (Epi-, Mono-, Iso-, Endo- und Automorphismus) existieren sinngemäß auch für Ringe ((Schief-)Körper).

Bemerkung: Sei $\varphi : R \to R'$ ein Ringhomomorphismus.

1. Offensichtlich ist eine Komposition von Ringhomomorphismen wieder ein Ringhomomorphismen.
2. $\ker\varphi \trianglelefteq R$ $\quad (1)\varphi(0) = 0, 2)a, b \in \ker\varphi : \varphi(a + b) = \varphi(a) + \varphi(b) = 0, 3)a \in \ker\varphi, b \in R : \varphi(ab) = \varphi(a)\varphi(b) = 0 \cdot \varphi(b) = 0)$

   $\mathrm{im}\varphi \leqslant R$ Unterring, i.A. kein Ideal!
3. $R^* =\{\, a \in R \,|\, \exists b \in R : ab = ba = 1 \,\}$ – Einheitengruppe.

   φ induziert einen Gruppenhomomorphismus: $\varphi^* : R^* \to {R'}^*, a \mapsto \varphi(a)$.
4. Ist R ein Körper, $R' \neq \{0\}$. Dann ist φ injektiv. (Angenommen φ ist nicht injektiv. Dann ist $\ker\varphi \neq \{0\} \trianglelefteq R$, d.h. $\ker\varphi = R \Rightarrow \perp$)

Sei $I \trianglelefteq R, R$ ein Ring. Ziel: Definiere auf $R/I = \{\, a + I \,|\, a \in R \,\}$ eine Ringstruktur.
Addition: $\forall a, b \in R : (a + I) + (b + I) = (a + b) + I$
Multiplikation: $\forall a, b \in R : (a + I) \cdot (b + I) = (a \cdot b) + I$
Dies ist wohldefiniert! In der Tat, seien $a', b' \in R$ mit $a + I = a' + I, b + I = b' + I$. Das heißt, dass $\exists i_a, i_b \in I : a = a' + i_a, b = b' + i_b$.
Zu zeigen: $a \cdot b + I = a' \cdot b' + I$.

$ab + I = (a' + i_a)(b' + i_b) + I = a'b' + \underbrace{a' \cdot i_b}_{\in I \text{ falls kommutativ}} + \underbrace{i_a b'}_{\in I} + \underbrace{i_a i_b}_{\in I} + I = a'b' + I$, da $I \trianglelefteq$

ÜA: $(R/I, +, \cdot)$ ist ein Ring und $\bar{\varphi} : R \to R/I, a \mapsto a + I$ ist ein surjektiver Ringhomomorphismus.
Wiederholung:
$I \triangleleft R : R/I = \{a + I | a \in R\}$. R/I Faktorring „R modulo I"
$\pi : R \to R/I, a \mapsto a + I$ surjektiver Ringhomomorphismus

Satz 8 (2.13) *Sei $\varphi : R \to R'$ Ringhomomorphismus und $I \trianglelefteq R$ derart, $I \subseteq \ker \varphi$. Dann existirt ein eindeutiger Ringhomomorphismus $\bar{\varphi} : R/I \to R'$ derart, dass*

$$\bar{\varphi} \circ \pi = \phi$$

und

- $im\varphi = im\bar{\varphi}$
- $\ker \bar{\varphi} = \pi(\ker \varphi)$
- $\ker \varphi = \pi^{-1}(\ker \bar{\varphi})$

Insbesondere ist $\bar{\varphi}$ injektiv gdw. $I = ker\varphi$

Korrolar 3 (2.14) *Ist $\varphi : R \to R'$ surjektiver Ringhomomorphismus (mit $I = \ker \varphi$), dann ist*

$$\bar{\varphi} : R/(\ker \phi) \to R'$$

Ringisomorphismus.

Isomorphisätze 1.20 und 1.21 haben Analoga in Ringtheorie („Gruppe"$leftrightarrow$ „Ring", „Normalteiler"$leftrightarrow$ „Ideal ").
Motivation: $I \triangleleft R \rightsquigarrow R/I$. **Ziel:** Gegeben ringtheoretische Eigenschaft P: „Was heisst es für I, dass R/I Eigenschaft P hat?".

Definition 20 (2.15) *Sei R Ring (kommutativ mit 1), $I \triangleleft R$, $I \neq R$. I heisst*

- *Primideal (prim) in R, falls gilt: $\forall a, b \in R : ab \in I \Rightarrow a \in I$ oder $b \in I$*
- *Maximalideal (maximal) in R, falls: $J \trianglelefteq R, I \subseteq J \Rightarrow I = J$ oder $J = R$ (informell: Es gibt kein echtes Ideal zwischen I und R. Aber vorsicht: nicht eindeutig!)*

In der Literatur: $\mathfrak{p}$ Prim, $\mathfrak{m}$ Maxi

Lemma 1 (2.16) *Seit $R \neq \{0\}$ Ring. Das Nullideal $\{0\}$ ist*

- *prim gdw. R IB ist*
- *max gdw R Körper ist*

Beweis:
@1: (0) ist prim: $a \cdot b \in (0) \Leftrightarrow ab = 0 \Rightarrow a \in (0) oder b \in (0) \Leftrightarrow a = 0$ oder $b = 0) \Leftrightarrow 0$ ist der einzige Nullteiler $\Leftrightarrow R$ ist IB.
@2: Angenommen (0) max in R. Zu zeigen: R Körper, das heisst $R^* = R \setminus \{0\}$. Sei $a \in R \setminus \{0\}$. Es reicht zu zeigen: $(a) = R = (1)$. Klar nach Maximalität des Nullideals (0).
Angenommen R ist Körper, So hat R nur die beiden(!) Ideale (0) und $(1) = R$. Damit ist (0) maximal. □
Beachte: $R \cong R/(0)$.

Proposition 1 (2.17) *Sei R ein Ring, $I \triangleleft R$, $(R \neq (0), I \neq R)$. Dann ist I*

1. *prim gdw. R/I ein IB ist.*
2. *maximal gdw. R/I ein Körper ist.*

*Insbesondere ist jedes **maximale Ideal** prim (Umkehrung gilt nicht!).*

Beweis:
$^{-}: R \to R/I; a \in R\bar{a} = a + I$; $x \in R : \bar{x} = \bar{0}$ gdw. $x \in I$
@1: I prim gdw. $\forall a, b \in R : (\bar{a} \cdot \bar{b} = \bar{ab} = \bar{0} \Rightarrow \bar{a} = \bar{0}$ oder $\bar{b} = \bar{0} \Leftrightarrow R/I$ ist IB $(x, y \in R/I, xy = 0 \Rightarrow x = 0$ oder $y = 0)$
@2: Nach Lemma 2.16 reicht zu zeigen: I maximal genau dann wenn in R/I das Nullideal maximal ist. Behauptung folgt aus der Tatsache, dass $\{J \lhd R | I \trianglelefteq J\} \leftrightarrow \{\bar{J} \lhd R/I\}$ mit $J \mapsto \bar{J} = \{\bar{j} | j \in J\}$ bijektiv ist.□

Korrolar 4 (2.18) *Ideale in* $(\mathbb{Z}, +, \cdot)$ *sind von der Fom* $m\mathbb{Z} = (m), m \in \mathbb{N}_0$.
(m) *ist* ***prim*** *genau dann wenn* $m = 0$ *oder* m *Primzahl.*
(m) *ist* ***maximal*** *genau dann wenn* m *Primzahl.*

Seien $a, b \in \mathbb{Z}$ heissen **koprim** (teilerfremd), wenn $ggT(a, b) = 1$: $\exists x, y \in \mathbb{Z} : ax + by = 1$ (Lemma von Bézout).
Idealtheoretisch formuliert: $(a) + (b) = (1) = \mathbb{Z}$ - Äquivalent zu Bézouts Lemma.
(Variante des) **Chinesichen Restsatzes**: Eine Kongruenz modulo $a \cdot b$ ist lösbar gdw. wenn sie lösbar ist $mod(a)$ und $mod(b)$.
Zum Beispiel $a = 2, b = 3$: $X^2 \equiv 5 mod(6)$ lösbar gdw. $X^2 \equiv 5 \equiv 1 mod(2)$ lösbar **und** $X^2 \equiv 5 \equiv 2 mod(3)$.
Letzteres ist aber nicht lösbar, also ist die Gleichung $mod(6)$ nicht lösbar.
R Ring $I_1, I_2 \trianglelefteq R$ koprim $:\Leftrightarrow I_1 + I_2 = R \Leftrightarrow (I_1, I_2) = 1$

Satz 9 (2.19) *Chinesischer Restsatz (Chinese Remainder Theorem (CRT)) Sei* R *kommutativer Ring mit 1,* $I_1, \ldots, I_n$ *paarweise koprime Ideale. Dann ist*

$$\varphi : R \to R/I_1 \times \cdots \times R/I_n, a \mapsto (a + I_1, \ldots, a + I_n)$$

ein surjektiver Ringhomomorphismus mit $\ker \varphi = \bigcap_{j=1}^{n} I_j =: S$.
Korrolar 1.24: $\bar{\varphi} : R/S \tilde{\to} R/I_1 \times \cdots \times R/I_j$ *ist Ringisomorphismus.*

Beweis:
Zeige Surjektivität von φ! Zeige zunächst: $\forall j \in [n] = \{1, 2, \ldots, n\} : I_j$ und $bigcap_{i \neq j} I_i$ sind koprim, das heisst, $1 \in I_j + \bigcap_{i \neq j} I_i$.
Nach Voraussetzung existieren für $i \neq j$ Elemente $a_i \in I_j, a'_i \in I_i$ mit $a_i + a'_i = 1$.

$$1 = \prod_{i \neq j} 1 = \prod_{i \neq j} (a_i + a'_i) \in I_j + \prod_{i \neq j} I_i \subseteq I_j + \bigcap_{i \neq j} I_i$$

.
TODO: REST IN VORLESUNG VOM 10.11.

2.2 Primfaktorzerlegung

Definition 21 (2.20) *Ein Integritätsbereich* R *heißt* ***euklidisch****, falls es eine* ***euklidische Normfunktion*** $n : R \setminus \{0\} \to \mathbb{N}_0$ *gibt, derart, dass* $\forall a, b \in R$*, mit* $a \neq 0, \exists q, r : b = qa + r$*, mit* $r = 0$ *oder* $n(r) < n(a)$.

Beispiel 2.21:

1. $\mathbb{Z}$ mit $n : \mathbb{Z} \setminus \{0\} \to \mathbb{N}_0, n(a) := |a|$.

2. Sei K ein Körper, $R = K[X], n : f \mapsto \deg f$.

Satz 10 (2.22) *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis: Sei R ein euklidischer Ring, $I \lhd R, (0) \neq I$. Es ist zu zeigen, dass I ein Hauptideal.
Wähle ein $a \in I \setminus \{0\}$ derart, dass $n(a)$ minimal ist. Es reicht zu zeigen, dass $I = (a)$.
„$\supseteq$“ klar.
„$\subseteq$“ Sei $b \in I, b = qa + r$. Ist $r = 0$, so ist $b \in (a)$. Ist $r \neq 0$, dann ist $n(r) < n(a)$. $(r = b - qa \in I)$. Widerspruch zur Wahl von a. □

Notation: Sei R ein Integritätsbereich. $x, y \in R$. Schreibe „$x \mid y$“ für „x teilt y“; d.h. $\exists c \in R, xc = y$; andernfalls „$x \nmid y$“.
Lemma [2.23]: Sei R ein Integritätsbereich. $x, y \in R$. Dann sind äquivalent:

1. $x \mid y$ und $y \mid x$

2. x und y sind assoziiert, d.h. $\exists c \in R^* : y = xc$

3. $(x) = (y)$

Definition 22 (2.24) *Sei R ein Integritätsbereich. Ein Element $x \in R \setminus (R^* \cup \{0\})$ heißt*

- ***irreduzibel***, *falls* $(\forall y, z \in R. x = yz \Rightarrow (y \in R^* \text{ oder } z \in R^*))$
- ***prim***, *falls* $(\forall y, z \in R\ x \mid yz \Rightarrow x \mid y \text{ oder } x \mid z)$.

i.a.W. (x) ist Primideal.

Satz 11 (2.25) *Sei R ein Hauptidealring, $x \in R \setminus (R^* \cup \{0\})$. Dann sind äquivalent:*

1. *(x) ist maximal*
2. *(x) ist Primideal, d.h. x ist prim.*
3. *x ist irreduzibel.*

Beweis:

- „$1 \Rightarrow 2$“: maximale Ideale sind prim. (Prop 2.17)
- „$2 \Rightarrow 3$“: x prim. Sei $x = yz$. Da x prim ist, gilt $x \mid y$ oder $x \mid z$. Angenommen $x \mid y$. Es existiert also $c \in R : y = cx$, also $x = czx$. Also $x(1 - cz) = 0, x \neq 0, R$ ist Integritätsbereich, d.h. $1 = cz$, d.h. $z \in R^*$.
- „$3 \Rightarrow 1$“: Sei x irreduzibel. Z.z.: (x) ist maximal. Sei dazu $x \in (x) \subseteq I = (a) \trianglelefteq R$. Wir wissen: $x \in (a)$, es existiert also $c \in R : x = ca$. Da x irreduzibel ist $c \in R^*$ oder $a \in R^*$. Wenn $c \in R^*$, so gilt $(x) = (a)$. Wenn $a \in R^*$, so gilt $(a) = R$. Also ist (x) maximal

□

Bemerkung: „$1 \Leftrightarrow 2$“ gilt in allgemeinen Integritätsbereichen (nicht notwendigerweise Hauptidealringe).

Beispiel 2.26: Allgemein: „prim $\Rightarrow$ irreduzibel“. In Hauptidealringen: „prim $\Leftrightarrow$ irreduzibel“. Im Allgemeinen gilt „irreduzibel $\Rightarrow$ prim “ nicht. Betrachte $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{-5}] = \{\, a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \,\}$
$g = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$.
Tatsache: $3, 2 \pm \sqrt{-5}$ sind irreduzibel, 3 ist allerdings nicht prim: $3 \mid 3^2$, aber $3 \nmid (2 \pm \sqrt{-5})$

Definition 23 (2.27) *Sei R ein Integritätsbereich. $a \in R$.*

1. *Eine **Zerlegung (Faktorisierung) von** a **in irreduzible Faktoren** ist eine Produktdarstellung der Form $a = e \cdot p_1 \cdot \dots \cdot p_r$, wobei $e \in R^*$, $p_1, \dots, p_r$ irreduzibel.*
2. *a hat eine **eindeutige** Faktorisierung in irreduzible Faktoren, falls aus $a = e' \cdot p'_1 \cdot \dots \cdot p'_s$ ($e' \in R^*$, irreduzibel Element p'_i) folgt, dass $r = s$ und - nach eventueller Umnummerierung - $(p_i) = (p'_i)$ für alle $i = 1, \dots, r$.*
3. *Ein Integritätsbereich, in dem jedes von 0 verschiedene Element eine **eindeutige** Faktorisierung in irreduzible Elemente hat, heißt **faktoriell** (factorial, unique factorization domain = UFD).*

Proposition 2 (2.28) *Sei R ein Integritätsbereich derart, dass jedes $a \in R \setminus \{0\}$ eine Faktorisierung in irreduzible Elemente besitzt. Dann ist äquivalent:*

1. *R ist faktoriell*
2. *Jedes irreduzible Element von R ist prim.*

Beweis: „$1 \Rightarrow 2$“: Seien $a, b \in R \setminus \{0\}$ mit $a = e_a p_1 \dots p_r, b = e_b q_1 \dots q_s, e_a, e_b \in R^*$, p_i, q_j irreduzible Elemente. Sei $p \in R$ irreduzibel mit $p \mid ab$. $p \mid \underbrace{e_a e_b \cdot p_1 \dots p_r q_1 \dots q_s}_{a \cdot b}$. Da R faktoriell ist, ist p assoziiert zu einem der p_i oder einem der q_j (d.h. $(p) = (q_j)$ oder $(p) = (p_i)$). Also $p \mid a$ oder $p \mid b$.
„$2 \Rightarrow 1$“: Angenommen $a = ep_1 \dots p_r = e'p'_1 \dots p'_s$. z.z.: $r = s$ und $(p_i) = (p'_i)$ nach Umnummerierung.
$e, e' \in R^*, p_i, p_j$ irreduzibel.
O.B.d.A. $r > 0$. $p_1 \mid e'p'_1 \dots p'_s$. Es existiert also ein $j \in [s] : p_1 \mid p'_j$. Das heißt $\exists c \in R : p'_j = P_1 c$, aber p_i, p'_j irreduzibel. Das heißt $c \in R^*$. Und das wiederum heißt $(p_1) = (p'_j)$.
$a = ep_1 \dots p_r = e' \cdot \underbrace{c \cdot p_1}_{=p'_j} \cdot p'_1 \dots \hat{p'_j} \dots p'_s$. RIB $\Rightarrow$ d.h. $ep_2 p_r = \underbrace{e'c}_{\in R^*} p'_1 \dots \hat{p'_j} \dots p'_s$
Rest per Induktion. □

Bemerkung: In einem faktoriellen Ring sind alle irreduziblen Elemente prim.

Satz 12 (2.29) *Jeder Hauptidealring ist faktoriell*

Beweis: Sei R ein Hauptidealring (insbesondere Itegritätsbereich). Nach Proposition 2.28 reicht zu zeigen:

1. Jedes Element in $R \setminus (R^* \cup \{0\})$ hat eine Zerlegung in irreduzible Faktoren
2. Jedes irreduzible Element in R ist prim.

@1: Sei $r \in R \setminus (R^* \cup \{0\})$. Ist r reduzibel, so existiert $c_1, r_1 \in R \setminus R^* : r = c_1 r_1$. Ohne Einschränkung ist r_1 reduzibel. Ist r_1 reduzibiel, so existieren $c_2, r_2 \in R \setminus R^* : r_1 = c_2 r_2$. Ist r_2 reduzibel, so existieren $c_3, r_3 \in R \setminus R^* : r_2 = c_3 r_3$. Terminiert dieser Prozess nicht, so existiert eine unendliche Folge von Elementen $r_1, r_2, r_3, ...$ mit $(r_1) \subsetneq (r_2) \subsetneq (r_3) \subsetneq \dots$. Beachte $I := \bigcup_{i=1}^{\infty} (r_i) \triangleleft R$.
R ist aber Hauptidealring $\Rightarrow r_\infty \in R : i = (r_\infty)$, insbesondere $r_\infty \in I$.
$\exists N : r_\infty \in (r_N)$, das heisst $I \subseteq (r_N)$. Widerspruch zur Aussage, dass $(r_N) \subsetneq (r_{N+1}) \subsetneq \dots$. Das heisst Hauptidealringe sind **noethersch** (Emmy Noether, 1882-1935).
@2: Sei $p \in R$ irreduzibel. Zu zeigen: p ist prim. Seien $a, b \in R$ mit $p \mid ab$ und $p \nmid b$. Zu zeigen: $p \mid b$.
$I := (a, p) = \{xa + yp | x, y \in R\} = (r)$ für $r \in R$, da R Hauptidealring ist.
Es gilt natürlich $r \mid a, r \mid p$, sagen wir $p = rc$ fur ein $c \in R$. Da p irreduzibel ist, dann ist entweder $r \in R^*$ oder $c \in R^*$. Ist $c \in R^*$, so gilt $(p) = (r)$. Widerspruch zu $\underbrace{p \nmid a}_{(p) \not\supseteq (a)}$, $\underbrace{r \mid a}_{(r) \supseteq (a)}$.
Also ist $r \in R^*$ und $I = R$. Es existiert also $x, y \in R : 1 = xa + yp$.
$p \mid ab \Rightarrow \exists c' \in R : pc' = ab$.
$b = 1 \cdot b = (xa + yb)b = x(ab) + p(yb) = p(c'x + yb) \Rightarrow p \mid b$. $\square$

Korrolar 5 (2.30)
1. *$\mathbb{Z}$ ist faktoriell : $a \in \mathbb{Z} \setminus \{0\} : a = \epsilon \prod_{p \in P} p^{v_p(a)}, v_p(a) \in \mathbb{N}_0, v_p(a) = 0$ für fast alle $p \in P$. P Menge aller Primzahlen, $\epsilon \in \{1, -1\}$. $v_p(a)$ sind eindeutig bestimmt. Dies nennt man auch die „p-adische Bewertung von a“*
2. *K Körper, $f \in K[X] \setminus \{0\}$. $f = c \cdot \prod_{g \in P} g^{v_g(f)}, c \in K^*$. P Repräsentatensystem der irreduziblen Polynome in $K[X]$ (Z.B. normierte irreduzible Polynome).*

Definition 24 (2.31) *Sei R Integritätsbereich, $a_1, \dots, a_r \in R$, Ein Element $t \in R$ heisst **gemeinsamer Teiler** (gT, common divisor) von $a_1, \dots, a_r$, wenn $t \mid a_i \forall i = 1, \dots, r$.*
*Ein gemeinsamer Teiler d von $a_1, \dots, a_r$ heisst **größter gemeinsamer Teiler** (ggT, greatest common divisor = gcd), falls $t \in R$ gemeinsamer Teiler von $a_1, \dots a_r \Rightarrow t \mid d$.*
*ÜA: **falls** ggT d existiert, so ist er eindeutig bis auf Assoziativität. Schreibe ggf. $d = ggT(a_1, \dots, a_r)$.*
***Analog:** $b \in R$ heisst **gemeinsames Vielfaches** (gV, common multiple) von $a_1, \dots, a_r$, falls $a_i \mid b$ für $i = 1, \dots, r$. Ein gemeinsames Vielfaches $c \in R$ heisst **kleinstes gemeinsames Vielfaches** (kgV, least common multiple) von $a_1, \dots, a_r$, falls $b \in R$ gemeinsames Vielfaches von $a_1, \dots, a_r \Rightarrow c \mid b$.*
Wieder: Ggfs ist $c = kgV(a_1, \dots, a_r)$ eindeutig bis auf Assoziativität.

Proposition 3 (2.32) *Sei R faktoriell, P Repräsentatensystem der irreduziblen Elemente $a_1, \dots, a_r \in R \setminus \{0\}$:*

$$\forall i \in [r] : a_i = \epsilon_i \prod_{p \in P} p^{v_p(a_i)}, \epsilon_i \in R^*, v_p(a_i) \in \mathbb{N}_{\not{0}}, \text{ für fast alle } v_p(a_i) = 0$$

so existieren ggT und kgV von $a_1, ..., a_r$ und

$$ggT(a_1, \dots, a_r) = \prod_{p \in P} p^{min\{v_p(a_i) | i = 1, \dots, r\}} \in R$$

$$kgV(a_1, \dots, a_r) = \prod_{p \in P} p^{max\{v_p(a_i) | i = 1, \dots, r\}} \in R$$

Beweis: $a \mid b \Leftrightarrow \forall p \in P : v_p(a) \leq v_p(b)$. $a = \epsilon_a \prod_p p^{v_p(a)}, b = \epsilon_b \prod_p p^{v_p(b)} \square$.

2.3 Lokalisierungen, Quotientenkörper, Satz von Gauß

Sei R Ring. $S \subseteq R$, multiplikativ abgeschlossen (Z.B. wenn R Integritätsbereich, $S = R \setminus \{0\}$ oder $\mathfrak{p} \triangleleft R$ prim, sei $S = R \setminus \mathfrak{p}$.
Setze $M = \{(a, b) | a \in R, b \in S\}$. Definiere Relation

$$(a, b) \sim (a', b') :\Leftrightarrow \exists c \in S : ab'c = a'bc \overset{R \text{ IB}}{\Leftrightarrow} ab' = a'b$$

(ÜA: Diese Relation ist eine Äquivalenzrelation). Schreibe $\frac{a}{b}$ für die Äquivalenzklasse, die (a,b) enthält.
Bemerkung: b ist hier nicht zwingend eine Einheit.
Schreibe $S^{-1}R(= R_S) = \{\frac{a}{b}|a \in R, b \in S\}$.
Dies ist ein Ring mit der durch „Bruchrechnung“ gegebenen Operation $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$. Homomorphismus $\varphi : R \to S^{-1}R, a \mapsto \frac{a}{1}$ “Lokalisierung von R an S“.
Wichtiger Spezialfall: Wenn R Integritätsbereich ist und $S = R \setminus \{0\}$.
$S^{-1}R = Q(R) = \{\frac{a}{b}|a, b \in R, b \neq 0\}$ **Quotientenkörper** von R (field of fractions). ($\frac{a}{b} \sim \frac{a'}{b'} :\Leftrightarrow b'a = ba'$)

Beispiel 2.34:

1. $R = \mathbb{Z}, Q(\mathbb{Z}) = \mathbb{Q}$
2. $R = \mathbb{Z}, p$ Primzahl, $S := \mathbb{Z} \setminus (p) \rightsquigarrow S^{-1}R =\{\, \frac{a}{b} \mid a \in \mathbb{Z}, p \nmid b \,\}$
3. $R = K[X], K$ ist ein Körper, $Q(K[X]) = K(X) =\{\, \frac{f(x)}{g(x)} \mid f, g \in K[X], gneq0 \,\}$
   „Körper der rationalen Funktionen in X über K“

z.B.: $f = X^2 + 1$. Wir wollen „$f = 0$“ lösen. Gegeben Ring R, bestimme $\{\, x \in R \mid f(x) = 0 \,\}$
$\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1}) =\{\, a + bi \mid a, b \in \mathbb{Q} \,\}$
$f \in \mathbb{Q}(i)[X] : f = (X - i)(X + i)$

Sei R (für den Moment) faktoriell und P Repräsentantensystem der irreduziblen Elemente von R (z.B.: in $\mathbb{Z} : P = \{$ Primzahlen $\})$.
$Q(R) \qquad x = \frac{a}{b} = \varepsilon \prod_{p \in P} p^{v_p(x)}$ (wobei $\varepsilon \in R^*$), $v_p(x) \in \mathbb{Z}, v_p(x) = 0$ für fast alle p.
z.B.: $R = \mathbb{Z}, x = \frac{4}{3} = (-1) \cdot \frac{2^2}{3} = (-1) \cdot 2^2 \cdot 3^{-1} \cdot 5^0 \cdot 7^0 \ldots.$
Setze $v_p(0) = \infty$ für $p \in P$. $v_2(x) = 2, v_3(x) = -1$

Definition 25 (2.35) *R, P wie oben. $f(X) = \sum_{i=0}^{\infty} a_I X^i \in Q(R)[X]$. Für $p \in P$ setze $v_p(f) := min \{\, v_p(a_i) \mid i \in \mathbb{N}_{\not 0} \,\}$ $\in \mathbb{Z} \cup \{\infty\}$. $f \in R[X]$ heißt **primitiv**, falls $v_p(f) = 0$ für alle $p \in P$.*
(d.h. ggT$(a_0, a_1, \ldots, a_n) = 1$ (a_i = von 0 verschiede Koeffizienten))

Lemma 2.36: (Gaußsches Lemma) R faktoriell, P wie oben, $p \in P$. Dann gilt, für $f, g \in Q(R)[X] : v_p(fg) = v_p(f) + v_p(g) \quad (*)$.
Beweis: Reduziere auf den Fall $f, g \in R[X]$, beide primitiv. o.B.d.A. $f, g \neq 0$. $(*)$ ist klar falls f oder g konstant sind (d.h. deg $= 0$).
$f(X) = \sum_i a_i X^i, a_i = \frac{c_i}{d_i}$
o.B.d.A. sind aber $f, g \in R[X]$, sogar primitiv.
Rzz: $v_p(fg) = 0$.
Betrachte $\varphi_p : R[X] \to R/(p)[X], \sum_{i=0}^{\infty} a_i X^i = f \mapsto \sum_{i=0}^{\infty} \bar{a}_i X^i, \bar{a}_i = a_i + (p) \in R/(p)$.
$\ker(\varphi_p) =\{\, f \in R[X] \mid v_p(f) > 0 \,\}$ (per Definition von $v_p(f)$!)
d.h. $g, f \notin \ker(\varphi_p)$.
$\varphi_p(fg) = \varphi_p(f)\varphi_p(g) \in R/(p)[X]$ ist ein IB!!! $\square$

Korollar (2.37): R faktoriell. $f, g \in R[X]$ primitiv $\Rightarrow fg \in R[X]$ primitiv.
Korollar (2.38): R faktoriell, $h \in R[X]$ normiert. Wenn $h = f \cdot g$ für normierte Polynome $f, g \in Q(R)[X]$. Dann sind bereits $f, g \in R[X]$. („wenn h über $Q(R)$ faktorisiert, dann schon über R.“)
Beweis: Für jedes $p \in P$ gilt $v_p(h) = 0$, $v_p(f), v_p(g) \leq 0$. Gauß: $v_p(h) = v_p(f) + v_p(g) = 0$.
d.h.: $v_p(f) = 0 = v_p(g)$, d.h.: $f, g \in R[X]$. $\square$

Satz 13 (2.39) *(Satz von Gauß) Ist R faktoriell, so ist auch $R[X]$ faktoriell. Die Primelemente von $R[X]$ sind von folgender Form:*

1. *Primelemente von R (betrachtet als konstante Polynome)*
2. *Primitive Polynome in $R[X]$, die Primelemente in $Q(R)[X]$ sind.*

z.B.: $R = \mathbb{Z} : p$ (p Primzahl), $f(= \sum_{i=0}^{\infty} a_i X^i) \in \mathbb{Z}[X]$. ggt$(a_i)$ = 1, f irreduzibel über $\mathbb{Q}$.

Beweis: Zeige zunächst, dass Polynome von Typ (1) und (2) prim sind.

1. Sei $q \in R$ prim. Z.z.: $qR[X] = (q) \triangleleft R[X]$ (”von q in $R[X]$ erzeugte Hauptideal”) ist prim.
   $R[X]/qR[X] \simeq \underbrace{R/qR}_{\text{IB!}}[X]$ – IB als Polynomring über IB R/qR.

2. $q \in R[X]$ primitiv, prim als Element von $Q(R)[X]$. zz.q prim als Elem...

   Seien also $f, g \in R[X]$ mit $q \mid f \cdot g$. Da q prim ist über $Q(R)$, teilt q eines der beiden Polynome, etwa f, d.h. $\exists h \in Q(R)[X].\ f = q \cdot h$. Lemma von Gauß: $\forall p \in P : v_p(f) = \underbrace{v_p(q)}_{=0} + v_p(h)$, d.h. $h \in R[X]$.

3 Übungsaufgaben

3.1 13/10/2014

Eindeutigkeit des Neutralen: Sei M ein Monoid. Zeige, dass $e \in M$ eindeutig ist.

Angenommen, es gäbe ein zweites neutrales Element e' mit $e \neq e'$. Dann würde gelten $e = e \cdot e' = e' \to \perp$ $\square$

Eindeutigkeit der Inversen: Sei M ein Monoid. Zeige, dass $a^{-1} \in M$, falls es existiert, eindeutig ist.

Angenommen, zu einem $a \in M$ gäbe es zwei inverse Elemente a', a'' mit $a' \neq a''$. Dann gilt $a' \cdot a \cdot a'' = a' \cdot e = a'$ als auch $(a' \cdot a) \cdot a'' = e \cdot a'' = a''$. Es folgt $a' = a'' \to \perp$ $\square$

3.2 15/10/2014

Aufgabe: Sei G eine Gruppe mit $g \in G$. Zeige: $\psi_g \coloneqq G \to G, h \mapsto ghg^{-1}$ ist ein Gruppenautomorphismus.