Satz 0.1. *Seien $\mathfrak{a} \subset A$, dann*

a) $\mathfrak{a}$ ist Primideal $\Leftrightarrow$ $A/\mathfrak{p}$ ist Integritätsbereich (nullteilerfrei)

b) $\mathfrak{a}$ ist maximales Ideal $\Leftrightarrow$ $A/\mathfrak{a}$ ist ein Körper.

Beweis. a) $\Rightarrow$ Sei $a + \mathfrak{a} \in A/p$ ein Nullteiler, dann existiert $x \in A \setminus p$, sodass

$$(a + \mathfrak{a})(x + \mathfrak{a}) = ax + \mathfrak{a} = p$$

Also ist $ax \in \mathfrak{a}$ und da $\mathfrak{a}$ Primideal folgt $a \in \mathfrak{a}$.

$\Leftarrow$ Sei $A/\mathfrak{a}$ Integritätsbereich und sei $ab \in \mathfrak{a}$, dann ist

$$(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a} = \mathfrak{a}$$

Da $A/\mathfrak{a}$ Integritätsbereich ist gilt $a + \mathfrak{a} = \mathfrak{a}$ oder $b + \mathfrak{a} = \mathfrak{a}$, also $a \in \mathfrak{a}$ oder $b \in \mathfrak{a}$.

b) $\Rightarrow$ Sei $I/\mathfrak{a}$ ein Ideal in $A/\mathfrak{a}$.
Hierbei ist I eine Ideal in A welches $\mathfrak{a}$ enthält, also $\mathfrak{a} \subseteq I \subseteq A$.
Da $\mathfrak{a}$ maximal ist, muss $\mathfrak{a} = I$ oder $\mathfrak{a} = A$. Also ist $A/\mathfrak{a}$ ein Körper.

$\Leftarrow$ Sei I ein Ideal in A mit $\mathfrak{a} \subseteq I \subseteq A$.
Dann ist $I/\mathfrak{a}$ eine Ideal in $A/\mathfrak{a}$, d.h.

$$I/\mathfrak{a} = \mathfrak{a}/\mathfrak{a} \quad \text{oder} \quad I/\mathfrak{a} = A/\mathfrak{a}$$

Damit folgt $I = \mathfrak{a}$ oder $I = \mathfrak{A}$.

□

Bemerkung. Insbesondere ist jedes maximale ideal prim.

Definition 0.2. Sei $A \neq \emptyset$. Eine **Relation** auf A ist eine Teilmenge $R \subset A \times A$. R heißt **partielle Ordnung** wenn

a) $\forall a \in A$ gilt $(a, a) \in R$ (Reflexivität)

b) $\forall a, b, c \in A$ gilt $(a, b) \in R$ und $(b, c) \in R$, so gilt auch $(a, c \in R)$ (Transitivität)

c) $\forall a, b \in A$ mit $(a, b \in R)$ und $(b, a) \in \mathbb{R}$, dann gilt $a = b$. (Antisymmetrie)

Ist R eine partielle Ordnungn auf A so schrieben wir für $(a, b) \in R$ auch $a \leq b$.
Zwei Elemente $a, b \in A$ heißen **vergleichbar**, wenn $a \leq b$ oder $b \leq a$ ist.
Eine Teilmenge $B \subset A$ heißt **Kette**, wenn für alle $a, b \in B$ gilt, dass $a \leq b$ oder $b \leq a$.

Lemma 0.3. *Sei $A \neq \emptyset$ partielle geordnet. Hat jede Kette $B \neq \emptyset$ in A eine obere Schranke in A, d.h. es gibt ein $a \in A$,sodass $b \leq a$ für alle $b \in B$., so besitzt A ein maximales Element.*

Theorem 0.4. *Sei $A \neq 0$ ein Ring, dann besitzt A ein maximales Ideal.*

Beweis. Sei $\Sigma = \{I \subset A \mid I \text{ ist Ideal}\}$. Dann ist $O \in \Sigma$ und Σ ist partielle geordnet durch die mengentheoretische Inklusion.
Sei $(C_i)_{i \in I}$ eine Kette in Σ. Dann ist

$$C = \bigcup_{i \in I} C_i$$

ein Ideal in A. Aus $I \notin C_i$ für alle $i \in I$ folgt, dass $I \notin C$,d.h. $C \in \Sigma$. Somit hat Σ ein maximales Element. $\square$

Korollar 0.5. *Sei A ein Ring und $I \subsetneq A$ ein Ideal, dann ist I in einem maximalen Ideal enthalten.*

Korollar 0.6. *Sei A ein Ring und $a \in A \setminus A^*$. Dann ist a in einem maximalen Ideal enthalten.*

Beweis. Betrachte $(a) = Aa \neq A$. $\square$

0.1 Lokale Ringe

Definition 0.7. Ein Ring A mit nur eine maximalen Ideal $\mathfrak{m}$ heißt **lokaler Ring** und $A/\mathfrak{m}$ heißt **Restklassenkörper** von A.

Satz 0.8. *Sei A ein Ring und $\mathfrak{m} \neq A$ eine Ideal in A.
Ist jedes $x \in A \setminus +m$ eine Einheit, si ist A ein lokaler Ring mit maximalen Ideal $\mathfrak{m}$.*

Beweis. Für jedes Ideal $I \subsetneq A$ gilt $I \cap A^* = \emptyset$, enthält also keine Einheiten und ist somit in $\mathfrak{m}$ enthalten. Somit ist $\mathfrak{m}$ das einzige maximale Ideal. $\square$

Satz 0.9. *Sei A ein Ring und $\mathfrak{m} \subset A$ eine maximales Ideal, sodass jedes Element m eine Einheit in A ist. Dann ist A ein lokaler Ring.*

Beispiel 0.10.1. Jedes Ideal in $\mathbb{Z}$ ist der Form $(m) = \mathbb{Z}m$ mit $m \in \mathbb{Z}_{\geq 0}$.
Es gilt, dass (m) genau dann Primideal ist, wenn $m = 0$ oder m Primzahl.
Ist $\mathfrak{p}$ Primzahl, so ist (p) maximal.

Sei K ein Körper und $A = K[X_1, ..., X_n]$. Dann ist der Kern des Homomorphismus $\phi : A \to K, f \mapsto f(0)$ ein maximales Ideal in A.

0.2 Radikale

Satz 0.11. *Sei A eine Ring und $N = \{a \in A \mid a \text{ ist nilpotent}\}$. Dann ist N ein Ideal in A und A/N enthält keine nilpotenten Elemente $\neq 0$.*

Beweis.
- Zz: N ist eine additive Untergruppe von A
  Seien $x, y \in N$ mit $x^n = y^m = 0$. Dann ist

  $$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k} = 0$$

  denn kann nicht sowohl $k < n$, als auch $n + m - k < m$ sein.

- Z.z. $AN \subset N$.
  Sei $x \in N$ mit $x^n = 0$ und $a \in A$. Dann ist $(ax)^n = a^n x^n = 0$, also $ax \in N$.
  Also ist N Ideal in A.
  Sei nun $a + N \in A/N$ nilpotent. Dann ist $(a+N)^n = 0$ für ein $n > 0$. Also ist $a^n + N = 0$, also $a^n \in N$.
  Dann ist $(a^n)^m = 0$ udn somit $a^{nm} = 0$, also nilpotent. Es folgt, dass $a \in N$.

$\square$

Definition 0.12. Das Ideal $N = \{a \in A \mid a \text{ ist Nilpotent}\}$ heißt das **Nilradikal** von A.

Definition 0.13. Sei A ein Ring dann nennt man $J = \{x \in A \mid \forall y \in A : 1 - xy \text{ ist Einheit}\}$ das **Jacobsonradikal**.

Satz 0.14. *Sei A eine Ring, dann ist*

a) das Nilradikal von A der Schnitt aller Primideal von A.

b) das Jacobsonradikal von A der Schnitt aller Maximalen Ideale von A.

Definition 0.15. Sei A ein Ring und $\mathfrak{a} \subset A$ ein Ideal in A. Dann wird

$$r(a) := \{x \in A \mid x^n \in \mathfrak{a} \text{ für ein } n > 0\}$$

als **Radikal** von $\mathfrak{a}$ bezeichnet. (auch $\mathrm{Rad}(\mathfrak{a})$, $\sqrt{\mathfrak{a}}$)

Beweis. Sei $\pi : A \to A/\mathfrak{a}$ die Kanonische Projektion. Dann ist $r(a) = \pi^{-1}\left(N_{A/\mathfrak{a}}\right)$. Also ist $r(a)$ ein Ideal. $\square$

Satz 0.16. *Sei $\mathfrak{a}, \mathfrak{b}$ ein Ideal, dann gilt*

a) $\mathfrak{a} \subseteq r(\mathfrak{a})$

b) $r\big(r(\mathfrak{a})\big) = r(\mathfrak{a})$

c) $r(\mathfrak{a}\mathfrak{a}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$

d) $r(\mathfrak{a}) = A \Leftrightarrow \mathfrak{a} = A$.

e) $r(\mathfrak{a} + \mathfrak{b}) = r\big(r(\mathfrak{a}) + r(\mathfrak{b})\big)$.

0.2.1 Operationen auf Radikalen

Definition 0.17. Sein A ein Ring.

a) Seien $\mathfrak{a}, \mathfrak{b} \subset A$ Ideale in A.
   Dann ist

$$a + b =: \{x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}$$

   ein Ideal in A.

b) Analog: Sei $(\mathfrak{a}_i)_{i\in I}$ eine Familie von Idealen in A, für eine Indexmenge I. Dann ist

$$\sum_{i\in I}\mathfrak{a}_i =: \left\{\sum_{i\in I} x_i \mid x_i \in \mathfrak{a}_i \text{ und fast alle } x_i = 0\right\}$$

ein Ideal in A.

c) Sei $(\mathfrak{a}_i)_{i\in I}$ eine Familie von Idealen in A, für eine Indexmenge I. Dann ist der Schnitt

$$\bigcap_{i\in I}\mathfrak{a}_i$$

ein Ideal in A.

d) Seien $\mathfrak{a}, \mathfrak{b} \subset A$ Ideal in A. Dann ist

$$\mathfrak{a}\mathfrak{b} = \left\{\sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, n \in \mathbb{N}\right\}$$

ein Ideal in A.

Satz 0.18. *Die Operationen Summe, Durchschnitt und Produkt auf Idealen sind kommutativ und Assoziativ und es gilt das Distributivgesetz.*

Definition 0.19. Sei A ein Ring. Zwei Ideale $\mathfrak{a}, \mathfrak{b} \subseteq A$ heißen **teilerfremd**, wenn $\mathfrak{a} + \mathfrak{b} = A = (1)$.

Satz 0.20. *Sei A ein Ring, $\mathfrak{a}, \mathfrak{b} \subset A$ Ideale in A. Dann sind äquivalent:*

a) $\mathfrak{a}, \mathfrak{b}$ sind Teilerfremd

b) Es gibt ein $x \in \mathfrak{a}, y \in \mathfrak{b}$, sodass $x + y = 1$.

Beweis. **2)⇒1)** Sei $z \in A$ und $x \in \mathfrak{a}, y \in \mathfrak{b}$, mit $x + y = 1$.
Dann ist $z = zx + zy$, wobei $zx \in \mathfrak{a}, zy \in \mathfrak{b}$, also $z \in \mathfrak{a} + \mathfrak{b}$.

1)⇒2)

□

Satz 0.21. *Sei A ein Ring und seinen $\mathfrak{a}_1, ..., \mathfrak{a}_n$ paarweise teilerfremde Ideal in A. Dann gilt*

a) Jedes $\mathfrak{a}_i$ ist teilerfremd zu $\prod_{\substack{j=1\\ j\neq i}}^{n}\mathfrak{a}_j$.

b) Es gilt

$$\prod_{i=1}^{n}\mathfrak{a}_i = \bigcap_{i=1}^{n}\mathfrak{a}_i$$

Beweis. a) Sei i fest. Es gibt Elemente $x_j \in \mathfrak{a}_i, y_j \in \mathfrak{a}_j$ mit $1 = x_j + y_j$ für $i \neq j$. Dann ist

$$1 = \prod_{\substack{j=1\\ j\neq i}}(x_j + y_j) = \underbrace{x}_{\in\mathfrak{a}_i} + \underbrace{\prod_{\substack{j=1\\ j\neq i}}}_{\in\prod_{\substack{j=1\\ j\neq i}}\mathfrak{a}_j} \in \mathfrak{a}_i + \prod_{\substack{j=1\\ j\neq i}}\mathfrak{a}_j$$

b) Durch Induktion über n.

$n = 2$ Sei $z \in \mathfrak{a} \cap \mathfrak{b}$. Schreieb $1 = x + y$ mit $x \in \mathfrak{a}, y \in \mathfrak{b}$. Dann ist $z = zx + zy \in \mathfrak{a}\mathfrak{b}$.

$n > 2$ Sei

$$\mathfrak{b} = \prod_{i=1}^{n-1} a_i$$

Wir nehmen an es gelte

$$\prod_{i=1}^{n-1} a_i = \prod_{i=1}^{n-1} \mathfrak{a}_i$$

Dann ist aber

$$\prod_{i=1}^{n} \mathfrak{a}_i = \mathfrak{a}_i \mathfrak{b}_i = \mathfrak{a}_i \cap \mathfrak{b} = \bigcap_{i=1}^{n} a_i$$

$\square$

Definition 0.22. Sei A ein Ring und seinen $\mathfrak{a}_i, ..., \mathfrak{a}_n$ Ideale in A.
Wir definieren die Abbildung

$$\phi : A \to \prod_{i=1}^{n} (A/\mathfrak{a}_i)$$
$$a \mapsto (a + \mathfrak{a}_1, ..., a + \mathfrak{a}_n)$$

Proposition 0.23. a) ϕ ist ein Ringhomomorphismus und

$$\text{Kern}(\phi) = \bigcap_{i=1}^{n} \mathfrak{a}_i$$

b) ϕ ist genau dann surjektiv, wenn die $\mathfrak{a}_i$ paarweise disjunkt sind.
Insbesondere ist

$$A/\prod_{i=1}^{n} \mathfrak{a}_i \simeq \prod_{i=1}^{n} A/\mathfrak{a}_i$$

Beweis. b) $\Rightarrow$ Sei ϕ surjektiv. Wir zeigen, dass $\mathfrak{a}_1$ und $\mathfrak{a}_2$ teilerfremd sind.
Es gibt ein $x \in A$ mit $\phi(x) = (1_{A/\mathfrak{a}_1}, 0, ..., 0)$.
Also ist $x = 1 \mod \mathfrak{a}_i$ und $x = x \mod \mathfrak{a}_2$.
Dann ist

$$1 = \underbrace{(1 - x)}_{\in \mathfrak{a}_i} + \underbrace{x}_{\in \mathfrak{a}_2} \in \mathfrak{a}_1 + \mathfrak{a}_2$$

$\Leftarrow$ Seien un die $\mathfrak{a}_i$ paarweise teilerfremd.
Es reicht zu zeigen,dass es Elemente $x_i \in A$ mit

$$\phi(x_i) = (0, ..., 0, 1, 0, ..., 0)$$

(1 an der i-ten Position) gibt.
Wir zeigen für $i = 1$:

Da $\mathfrak{a}_1 + \mathfrak{a}_j = A$ für alle $j > 1$, gibt es $x_j \in \mathfrak{a}_1, y_j \in \mathfrak{a}_j$ mit $x_j + y_j = 1$
Sei nun

$$x := \prod_{i=2}^{n} y_j = \prod_{i=2}^{n} 1 - x_j = 1 \mod \mathfrak{a}_1$$

und $x = 0 \mod \mathfrak{a}_j$ für $j > 1$.

□

0.3 Ringe von Brüchen

Definition 0.24. Sei A ein Ring. Eine Teilmenge $S \subset A$ heißt **multiplikativ abgeschlossen**, wenn

a) Für alle $s, t \in S$ gilt, dass $st \in S$

b) $1 \in S$.

Bemerkung 0.25. Auf $A \times S$ wird durch

$$(a, s) \sim (b, t) \Leftrightarrow (at - bs)u = 0 \text{ für ein } u \in S$$

eine Äquivalenzklasse definiert.
Für die Transitivität wird die multiplikative Abgeschlossenheit von S benötigt.
Die Äquivalenzklassen von (a, s) wird mit a/s bezeichnet.
Die Menge der Äquivalenzklasssen wir als $S^{-1}A$ geschrieben.

Definition 0.26. Seien $a/s, b/t \in S^{-1}A$. Man definiert

- $a/s + b/t := (at + bs)/st$
- $a/s \cdot b/t := ab/st$

Definition 0.27. Diese Verknüpfungen sind wohldefiniert und versehen $S^{-1}A$ mit einer Ringstruktur.
$S^{-1}A$ wird als der **Ring der Brüche** von A bezüglich S bezeichnet.

Beispiel 0.28. Sei $A = \mathbb{Z}$ und $S = \mathbb{Z} \setminus \{0\}$. Dann ist $S^{-1}A$ isomorph zu $\mathbb{Q}$.

Korollar 0.29. *Die Abbildung*

$$\begin{aligned} \varphi_S : A &\to S^{-1}A \\ a &\mapsto a/1 \end{aligned}$$

hat folgende Eigenschaften:

a) φ_S ist ein Ringhomomorphismus. (i.A. nicht injektiv)

b) Sei $s \in S$, dann ist $\varphi_S(s)$ eine Einheit in $S^{-1}A$.

c) $\mathrm{Kern}(\varphi_S) = \{a \in A \mid as = 0$ *für ein* $s \in S\}$.

d) Jedes Element in $S^{-1}A$ ist der Form $\varphi_S(a)\varphi_S(s)^{-1}$ für ein $a \in A$, $s \in S$.

Beweis. b) Sei $s \in S$, dann ist $s/1 \cdot 1/s = s/s = 1/1 = 1_{S^{-1}A}$

c) Sei $a \in \mathrm{Kern}(\varphi_S)$, dann ist $a/1 = 0/1$, also $(a1 - 01)s = 0$ für ein $s \in S$.
Also ist $as = 0$ für ein $s \in S$.

d) Sei $a/s \in S^{-1}A$. Dann ist

$$\varphi_S(a) = a/1 \qquad \varphi_S(s) = s/1 \qquad \varphi_S(s)^{-1} = 1/s$$

Es folgt

$$\varphi_S(a)\varphi(s)^{-1} = a/1 \cdot 1/s = a/s$$

□

Satz 0.30. *Seien A, B Ringe und $S \subset A$ multiplikativ abgeschlossen. Sei $g : A \to B$ ein Ringhomomorphismus, der 1)-3) aus erfüllt, dann gibt es einen eindeutigen Isomorphismus $h : S^{-1}A \to B$ mit $h \circ \varphi_S = g$.*

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "\varphi_S"] & B \\ S^{-1}A \arrow[ur, "h"'] & \end{tikzcd}$$

Definition 0.31. Sei A ein Integritätsbereich und $S = A \setminus \{0\}$. Dann nennt man $S^{-1}A$ den **Quotientenkörper**

Lemma 0.32. *Der Quotientenkörper ist ein Körper, φ_S ist injektiv und wir können A mit seinem Bild in $S^{-1}A$ identifizieren.*

Definition 0.33. Sei A ein Ring. Sei $\mathfrak{p}$ ein Primideal in A. Man schreibt $A_{\mathfrak{p}}$ für $S^{-1}A$ und nennt $A_{\mathfrak{p}}$ die **Lokalisierung** von A bezüglich $\mathfrak{p}$.

Lemma 0.34. *Sei A ein Ring. Sei $\mathfrak{p}$ ein Primideal in A.*
Dann ist $S = A \setminus \mathfrak{p}$ multiplikativ Abgeschlossen.

Lemma 0.35. *Sei $A = \mathbb{Z}$ und $p \in \mathbb{Z}$ eine Primzahl. Dann ist $\mathbb{Z}_{(p)} = \{m/n \mid m/n \in \mathbb{Q}, p \nmid n\}$.*

Satz 0.36. *Sei A ein Ring und $S \subset A$ multiplikativ abgeschlossen. Dann ist*

a) Ist I ein Ideal in A so ist auch $S^{-1}I = \{a/s \mid a \in I\}$ ein Ideal in $S^{-1}A$

b) Die Ideale in $S^{-1}A$ sind der Form $S^{-1}I$, wobei I ein Ideal in A ist.

c) Sind I, J Ideal in A, dann gilt

$$\begin{aligned} S^{-1}(I + J) &= S^{-1}I + S^{-1}J \\ S^{-1}(I \cap J) &= S^{-1}I \cap S^{-1}J \\ S^{-1}(IJ) &= (S^{-1}I)(S^{-1}J) \end{aligned}$$

Beweis. Wir beweisen nur 2).
Sei J ein Ideal in $S^{-1}A$. Dann ist $I = \varphi_S^{-1}(J)$ ein Ideal in A und $J = S^{-1}I$:
Sei $a/s \in S^{-1}I$. Aus $I = \varphi_S^{-1}(J)$ folgt, dass $\varphi_S(a) \in J$. Also ist

$$a/s = \underbrace{a/1}_{\varphi_S(a)} \cdot \underbrace{1/s}_{\in S^{-1}A} \in J$$

d.h. $s \in \varphi_S^{-1}(J) = I$ und $a/s \in S^{-1}I$. □

0.4 Integritätsbereiche und Hauptidealringe

Definition 0.37. Sei A ein Ring. Ein Ideal der Form $(a) = Aa$ heißt **Hauptideal**.

Definition 0.38. Ein Ring A heißt **Hauptidealring**, wenn jede Ideal in A Hauptideal ist.

Definition 0.39. Ein Ring A heißt **euklidisch**, wenn es eine Abbildung

$$\lambda : A \setminus \{0\} \to \mathbb{N}_0$$

gibt, sodass zu je zwei Elementen $a, b \in A$ mit $b \neq 0$ Elemente $q, r \in A$ existieren mit $a = qb + r$ wobei $\lambda(r) < \lambda(b)$ oder $r = 0$.

Beispiel 0.40. a) $\mathbb{Z}$ ist euklidisch unter $\lambda(x) = |x|$.

b) Sei K ein Körper. Dann ist $K[X]$ euklidisch mit $\lambda(f) = \deg(f)$.

Satz 0.41. *Sei A ein euklidischer Ring. Dann ist A ein Hauptidealring.*

Beweis. Sei $\mathfrak{a} \neq 0$ in Ideal in A. Dann hat

$$\lambda(x) \mid x \in a, x \neq 0$$

ein kleinstes Element, d.h. es gibt ein $x \in \mathfrak{a} \setminus \{0\}$ mit $\lambda(x) \leq \lambda(y)$ für alle $y \in \mathfrak{a} \setminus \{0\}$.
Es gilt $\mathfrak{a} = (x)$.
Sei $y \in a \setminus \{0\}$. Schreibe $y = qx + r$ mit $r = 0$ oder $\lambda(r) < \lambda(x)$.
Dann ist $r \in \mathfrak{a}$ und aus der Minimalität von $\lambda(x)$ folgt $r = 0$ und damit $\mathfrak{a} \subset (x)$. □

Definition 0.42. Sei A ein Ring und seinen $a, b \in A$.
$d \in A$ heißt **Größter gemeinsamer Teiler** von a und b, wenn gilt

a) $d|a$ und $d|b$.

b) Wenn es $g \in A$ gibt mit $g|a$ und $g|b$, dann muss $g|d$.

Wir schreiben $d = \gcd(a, b) = (a, b)$

Definition 0.43. Sei A ein Ring und seinen $a, b \in A$.
$d \in A$ heißt **kleinstes gemeinsames Vielfaches** von a und b, wenn gilt

a) $a|v$ und $b|v$.

b) Wenn es $g \in A$ gibt mit $a|g$ und $b|g$, dann muss $v|v$.

Wir schreiben $v = \operatorname{lcm}(a, b) = (a, b)$

Satz 0.44. *Sei A ein Hauptidealring und seien $a, b \in A$.*
Dann existiert ein $d = \gcd(a, b)$ und $v = \operatorname{lcm}(a, b)$ von a, b und es gilt

a) $(a) + (b) = (d)$

b) $(a) \cap (b) = (v)$

Beweis.

- Da A ein Hauptidealring ist, gilt $(a) + (b) = (d)$ für ein $d \in A$.
  Es gilt $a, b \in (d)$, also $d|a$ und $d|b$.
  Sei $g \in A$ mit $g|a$ und $g|b$. Dann ist $(a) \subset (g)$ und $(b) \subset (g)$.
  Daraus folgt, dass $(a) + (b) \subseteq (g)$, also $(d) \subset (g)$. Damit folgt $g|d$.
- Analog für lcm.

□

Definition 0.45. Sei A in Integritätsbereich. Zwei Elemente $a, b \in A$ heißen **assoziiert**, wenn

- $a|b$ und $b|a$.
- (äquivalent) $a = bu$ für ein $u \in A^*$.
- (äquivalent) $(a) = (b)$.

Man schreibt dann $a \sim b$.

Definition 0.46. Sei A in Integritätsbereich. Ein Element $p \in A$ heißt **prim**, **Primelement**, wenn

- $p \notin A^*$, $p \neq 0$ und aus $p|ab$ folgt $p|a$ oder $p|b$.
- (äquivalent) $p \neq 0$ und (p) ist Primideal.

Definition 0.47. Sei A in Integritätsbereich. $c \in A$ heißt **irreduzibel** oder **unzerlegbar**, wenn

a) für $c \notin A^*$ und $c \neq 0$ aus $c = ab$ folgt, dass $a \in A^*$ oder $b \in A^*$.

b) (äquivalent) für $c \neq 0$ für alle $a \in A$ gilt, dass aus $(c) \subset (a)$ folgt, dass $(a) = A$ oder $(a) = (c)$.

Satz 0.48. *Sei A ein Integritätsbereich und $p \in A$ prim. Dann ist p irreduzibel.*

Beweis. Sei $p = ab$, dann gilt $p|ab$. Es folgt $p|a$ oder $p|b$.
Angenommen $p|a$, dann ist $a = px$ für ein $x \in A$ und $p = pxb$. Es folgt, dass $p(1 - bx) = 0$ und da A Integritätsbereich ist $1 - bx = 0$.
Also muss $bx = 1$ also ist $b \in A^*$. □

Satz 0.49. *Sei A ein Hauptidealring und Integritätsbereich. Dann gilt für $c \in A$*

$$c \text{ prim} \Leftrightarrow c \text{ irreduzibel}$$

Beweis. Sei c irreduzibel, also ist (c) maximal. Daraus folgt, dass (c) Primideal ist und somit c prim. □

Definition 0.50. Ein Integritätsbereich heißt **faktoriell**, wenn

a) Jedes $a \in A \backslash A^*$, $a \neq 0$ zerfällt in ein Produkt von irreduziblen Elementen.

b) Die Zerlegung ist bis auf Reihenfolge und Einheiten eindeutig. D.h.

D.h. wenn $a = c_1 \cdot ... \cdot c_m = d_1 \cdot ... \cdot d_n$ mit c_1, d_1 irreduzibel, so folgt $m = n$ und es gibt $\pi \in S_n$ mit $c_1 \sim d_{\pi(i)}$ für alle $i = 1, ..., n$.

Bemerkung 0.51. Die Eindeutigkeit der Faktorisierung impliziert, dass es irreduzibles Element in einem faktoriellen Integritätsbereich prim ist.

Lemma 0.52. *Sei A ein Hauptidealring und S eine nichtleere Menge von Idealen in A. Dann hat S ein maximales Element (bezüglich $\subset$)*

Beweis. Angenommen S hat kein maximales Element. Dann gibt es zu jedem $\mathfrak{a}_1 \in S$ ein $\mathfrak{a}_2 \in S$ mit $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2$. Es gibt also eine unendliche Kette

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq ...$$

von Idealen in S. Sei nun $\mathfrak{a} := \bigcup_{j=1}^{\infty} \mathfrak{a}_i$.
Dann ist a ein Ideal in A, also ist $\mathfrak{a}$ ein Hauptideal und $\mathfrak{a} = (x)$ für ein $x \in A$.
Dann folgt insbesondere, dass $x \in \mathfrak{a}$. Damit folgt, dass es $j_0 \in \mathbb{N}$ gibt, mit $x \in \mathfrak{a}_{j_0}$.
Somit ist $(x) \subset \mathfrak{a}_{j_0}$ und somit $\mathfrak{a} = \mathfrak{a}_{j_0}$.
Dies bedeutet aber, dass die Kette stationär wird, was ein Widerspruch zur Annahme ist. □

Theorem 0.53. *Sei A ein Integritätsbereich. Ist A ein Hauptidealring, so ist A faktoriell.*

Beweis. **Zerlegbarkeit der Elemente** Sei $S = \{(a) \mid a \in A, a \notin A^*, a \neq 0$a zerfällt nicht in irreduzible Faktoren$\}$.
Angenommen $S \neq \emptyset$. Dann hat S eine maximales Element (a) und a ist nicht irreduzibel.
Dann gibt es $b, c \in A \setminus A^*$, mit $a = bc$.
Also ist $(a) \subsetneqq (b)$ und $(a) \subsetneqq (c)$. Da (a) maximal in S ist folgt daraus, dass $(b), (c) \notin S$.
Somit zerfallen b, c in irreduzible Faktoren und damit gilt $a \in S$. Widerspruch!.

Eindeutigkeit der Zerlegung Sei $a \in A$. Angenommen es gäbe zwei irreduzible Zerlegungen $a = c_1...c_m = d_1...d_n$ mit $m \leq n$.
Dann ist c_1 irreduzibel und somit prim. Also muss $c_1 | d_i$ für ein i gelte.
Nach Umnummerierung gilt $c_1 | d_1$, also $d_1 = u_1 c_1$ für $u_1 \in A^*$.
Also ist

$$\begin{aligned} & c_1...c_m = u_1 c_1 d_2 ... d_n \\ \Rightarrow \quad & c_2...c_m = d_2...d_n \end{aligned}$$

Fortsetzen des Argumentes liefert

$$1 = u_1...u_m d_{m+1}...d_n$$

für geeignete $u_i \in A^*$.
Dann sind aber $d_{m+1}, ..., d_n$ Einheiten und damit Eindeutig bis auf Einheiten und Reihenfolge.

□

0.5 Inverse und direkte Limiten

Definition 0.54. Man nennt I eine unter $\leq$ partiell geordnete Menge, wenn für alle $x, y, z \in I$ gilt

a) $x \leq x$.

b) Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$.

c) Aus $x \leq y$ und $y \leq x$ folgt $x = y$.

Definition 0.55. Für jedes $i \in I$sei A_i ein Ring und sei für jedes Paar $i, j \in I$ mit $i \leq j$ die Abbildung $f_{ij} : A_j \to A_i$ ein Ringhomomorphismus, sodass

a) $f_{ii} = \mathrm{id}_{A_i}$ für alle $i \in I$

b) $f_{ik} = f_{ij} \circ f_{jk}$ falls $i \leq j \leq k$.

Dann nennt man das System $(A_i, f_{ij})_{i,j \in I}$ **projektives System** von Ringen.

Definition 0.56. Ein Ring A zusammen mit dem Homomorphismus $f_i : A \to A_i$, sodass $f_i = f_{ij} \circ f_j$ für $i \leq j$ heißt **projektiver Limes** oder **inverser Limes** des Systems (A_i, f_{ij}), wenn folgende universelle Eingenschaft erfüllt ist:
Sind $h_u : B \to A_i$ für alle $i \in I$ Ringhomomorphismen mit $h_i = f_{ij} \circ h_j$ für $i \leq j$, so existiert genau ein Ringhomomorphismus $h : B \to A$ mit $h_i = f_i \circ h$ für alle $i \in I$.

$$\begin{tikzcd}
B \arrow[rr, "\exists! h"] \arrow[dr, "h_j"] \arrow[ddr, "h_i"'] & & A \arrow[dl, "f_j"'] \arrow[ddl, "f_i"] \\
& A_j \arrow[d, "f_j"] & \\
& A_i &
\end{tikzcd}$$

Bemerkung 0.57. Falls ein projektiver Limes existiert, so ist er bis auf kanonische Isomorphie eindeutig:
Sind (A, f_i) und (B, h_i) projektive Limiten von (A_i, f_{ij}), so gibt es Homomorphismen $h : B \to A$ und $g : A \to B$, die die oben beschrieben Verträglichkeitsbedingungen erfüllen.
Durch Zusammensetzen dieser Homomorphismen erhalten wir Abbildungen Die Eindeutigkeitsbedingung Impliziert nun, dass $g \circ h = \mathrm{id}_B$ und $h \circ g = \mathrm{id}_A$.
Man schreibt auch $A = \varprojlim_{i \in I} A_i$ für den projektiven Limes des Systems (A_i, f_{ij}).

Existenz des Projektiven Limes. Sei $(A_i, f_{ij})_{i,j \in I}$ ein projektives System von Ringen.
Setze

$$A = \left\{ (x_i)_{i \in I | f_{ij}(x_j) \,=\, x_i \text{ für } i \,\leq\, j} \right\} \subset \prod_{i \in I} A_i$$

und $h_j : A \to A_j, (x_i)_{i \in I} \mapsto x_j$.
Dann ist $(A, h_i)_{i \in I}$ ein projektiver Limes von (A_i, f_{ij}).
Insebsondere definiert jede Famiele $(x_i)_{i \in I}$ mit $f_{ij}(x_j) = x_i$ ein eindeutiges Element $x \in \varprojlim_{i \in I} A_i$. $\square$

Beispiel 0.58. Ein Beispiel für einen projektiven Limes sind die p-adisches ganzen Zahlen.
Sei $p \in \mathbb{Z}$ eine Primzahl, $I = \mathbb{N}$, mit der Ordnung $\leq$.
Für $n \geq 1$ sei $A_n = \mathbb{Z}/p^n\mathbb{Z}$. Sei

$$\begin{aligned} f_{mn} : A_n = \mathbb{Z}/p^n\mathbb{Z} &\to A_m = \mathbb{Z}/p^m\mathbb{Z} \\ x &\mapsto x \mod p^m \end{aligned}$$

Dann ist $(A_m, f_{mn})_{m,n\geq 1}$ ein projektives System. Der projektive Limes wird als Ring der p-adischen ganzen Zahlen

$$\mathbb{Z}_p = \varprojlim_{n\geq 1} A_n$$

bezeichnet. Also ist

$$\begin{aligned} \mathbb{Z}_p &= \{(x_n)_{n\geq 1} \mid x_n \in \mathbb{Z}/p^n\mathbb{Z}, f_{mn}(x_n) = x_n \text{ für } m \leq n\} \\ &= \{(x_n)_{n\geq 1} \mid x_n \in \mathbb{Z}/p^n\mathbb{Z}, x_n \mod p^{n-1} = x_{n-1}\} \end{aligned}$$

Wir schreiben die Elemente aus $\mathbb{Z}_p$ auch als Folgen

$$x = (x_n)_{n\geq 1} = (..., x_{n+1}, x_n, ..., x_1)$$

mit $x_n \mod p^{n-1} = x_{n-1}$.
Addition und Multiplikation erfolgen komponentenweise.
Sie Abbildung

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}_p \\ m &\mapsto (..., m + p^n, ..., m + p) \end{aligned}$$

ist in injektiver Ringhomomorphismus.