WS 2001/2

Zusätze zu Teil I.

A. Der Hilbert'sche Basissatz.

Wir betrachten im ersten Teil der Vorlesung vor allem endlich-erzeugte kommutative k-Algebren betrachten. Von Bedeutung ist die folgende Eigenschaft dieser endlich erzeugten, kommutativen k-Algebren: sie sind 'noethersch'. Diese Begriffsbildung soll auch für nicht notwendig kommutative Ringe vorgestellt werden, dort unterscheiden man zwischen 'links-noethersch' und 'rechts-noethersch'.

Ist R ein (nicht notwendig kommutativer) Ring, so nennt man eine nicht-leere Teilmenge L von R ein *Linksideal*, falls die folgenden beiden Eigenschaften gelten:
(1) (Abgeschlossenheit unter der Addition): Sind $x_1, x_2 \in I$, so ist auch $x_1 + x_2 \in I$.
(2) Ist $x \in I$ und $r \in R$, so gehört auch rx zu I.

Ist L ein Linksideal, so ist L eine Untergruppe von $(R, +)$, denn mit x gehört wegen der Bedingung (2) auch $-x = (-1)x$ zu L.

Eine Kette $\mathcal{I}$ von Linksidealen heißt *aufsteigend*, wenn es zu jedem $I \in \mathcal{I}$ nur endlich viele Ideale $I' \in \mathcal{I}$ mit $I' \subset I$ gibt.

Sei L ein Linksideal. Eine Teilmenge $S \subseteq L$ heißt *Erzeugendensystem von L*, falls jedes Element aus L eine (endliche) Summe $\sum r_i s_i$ mit $r_i \in R, s_i \in S$ ist; in diesem Fall schreiben wir $L = \sum RS$. Ist $S = \{s_1, \dots, s_n\}$ eine endliche Menge, so schreibt man natürlich auch $L = \sum_{i=1}^n Rs_i$. Besitzt L ein endliches Erzeugensystem, so heißt L *endlich erzeugt.*

Lemma. *Sei R ein Ring. Die folgenden Aussagen sind äquivalent:*
(i) *Jedes Linksideal von R ist endlich erzeugt.*
(i$'$) *Jedes Erzeugendensystems eines jeden Linksideals von R enthält ein endliches Erzeugendensystem.*
(ii) *Ist $\mathcal{I}$ eine nicht-leere Menge von Linksidealen von R, so gibt es in $\mathcal{I}$ ein maximales Element.*
(iii) *Jede aufsteigende Kette von Linksidealen von R ist endlich.*

Wenn diese Bedingungen erfüllt sind, so heißt R *links-noethersch*; man sagt in diesem Fall auch, daß *jede aufsteigende Kette abbricht,* und nennt dies die *aufsteigende Kettenbedingung.* (Ist R kommutativ und erfüllt diese Bedingungen, so nennt man ihn *noethersch*).

Beweis der Äquivalenz: (i) $\implies$ (iii): Angenommen es gibt eine aufsteigende Kette von Linksidealen, die nicht abbricht:

$$L_0 \subset L_1 \subset \dots \subset L_s \subset L_{s+1} \subset \dots$$

Sei $L = \bigoplus_{j \in \mathbb{N}_0} L_j$. Dies ist ein Linksideal, also endlich erzeugt. Sei etwa $L = \sum_{i=1}^t Rx_i$ mit $x_i \in L$. Jedes dieser Elemente x_i gehört zu L, also zu einem $L_{j(i)}$ mit $j(i) \in \mathbb{N}_0$. Ist s das Maximum von $j(1), \dots, j(t)$, so liegen alle x_i in L_s, es ist also $L \subseteq L_s$. Dies widerspricht aber der Tatsache, daß L_s eine echte Teilmenge von $L_{s+1} \subseteq L$ ist.

(iii) $\implies$ (ii): Offensichtlich.

(ii) $\implies$ (i$'$): Sei L ein Linksideal von R, sei S ein Erzeugendensystem von L. Sei $\mathcal{I}$ die Menge der Linksideale der Form $\sum RS'$, wobei S' eine endliche Teilmenge von S ist. Die Menge $\mathcal{I}$ ist nicht leer, da sie insbesondere das Nullideal $0 = \sum R\emptyset$ enthält. Wegen (ii) besitzt $\mathcal{I}$ ein maximales Element, etwa $L_0 = \sum RS_0$, dabei ist S_0 eine endliche Teilmenge von S. Ist nun $s \in S$, so ist auch $L_0 + Rs = \sum R(S_0 \cup \{s\})$ in $\mathcal{I}$ Linksideal von R. Wegen $L_0 \subseteq L_0 + Rs$ und der Maximalität von L_0 folgt $s \in L_0$. Wir sehen also: $L_0 = L$.

Hilbert'scher Basissatz. *Ist R links-noetherscher Ring, so ist auch $R[X]$ links-noetherscher Ring.*

Die Bezeichnung *Basissatz* ist eigentlich irreführend, denn nach gängiger Terminologie ist dies nicht ein Satz über "Basen", sondern über Erzeugendensysteme. Aber die Bezeichnung hat sich eingebürgert.

Beweis: Sei L ein Linksideal von $R[X]$, das nicht endlich erzeugt ist. Sei f_1 ein Polynom kleinsten Grades in $L \setminus 0$. Induktiv wähle als f_{m+1} ein Polynom kleinsten Grades in $L \setminus \sum_{i=0}^{m} R[X]f_i$. Sei n_m der Grad von f_m, sei r_m der höchste Koeffizient von f_m. Es ist $n_1 \leq n_2 \leq \dots$. Betrachte die Kette von Linksidealen $Ra_1 \subseteq Ra_1 + Ra_2 \subseteq \dots$. Behauptung: dies ist eine echt aufsteigende Kette. Wäre nämlich $a_{m+1} \in \sum_{i=1}^{m} Ra_i$, also $a_{m+1} = \sum_{i=1}^{m} r_i a_i$, mit $r_i \in R$, so ist

$$g = f_{m+1} - \sum_{i=1}^{m} r_i X^{n_{m+1}-n_i} f_i \quad \in \quad L \setminus \sum_{i=0}^{m} R[X]f_i$$

ein Polynom kleineren Grads als f_{m+1}, im Widerspruch zur Auswahl von f_{m+1}.

Mit Induktion erhält man: *Ist R links-noetherscher Ring, so ist auch jeder Polynomring $R[X_1, \dots, X_n]$ in endlich vielen Variablen links-noetherscher Ring.*

Betrachtet man Rechtsideale statt Linksideale, so erhält man den analogen Begriff eines rechts-noetherschen Rings (hier gilt also: jedes Rechtsideal ist endlich erzeugt); ist R kommutativer Ring, so sind die Linksideale genau die Rechtsideale und man nennt sie die Ideale von R; statt 'links-noethersch' sagt man in diesem Fall einfach 'noethersch': *Ist R ein noetherscher kommutativer Ring, so ist jeder Polynomring $R[X_1, \dots, X_n]$ in endlich vielen Variablen wieder ein noetherscher Ring.* Insbesondere gilt also: *Ist k ein Körper, so ist jeder Polynomring $k[X_1, \dots, X_n]$ in endlich vielen Variablen ein noetherscher Ring.*

B. Algebraische Mengen und die Zariski-Topologie.

Anwendung auf Nullstellenmengen von Polynomen. Sei k ein Körper, betrachte den affinen Raum k^n (für ein n). Im k^n interessieren uns die Nullstellenmengen $V(P)$ einer Menge von Polynomen. **Folgerung des Hilbert'schen Basissatzes:** *Zu jeder Menge $P \subseteq k[X_1, \dots, X_n]$ gibt es eine* **endliche** *Teilmenge $P' \subseteq P$ mit $V(P) = V(P')$.*

Nebenbemerkung. Man kann also jedes P durch eine endliche Teilmenge P' ersetzen. Kann man etwas sagen, wie klein man P' machen kann? Verwendet man die hier gegebene Formulierung, so kann P' beliebig groß sein, schon im Fall $n = 1$: Seien $a_1, \dots, a_m$ paarweise verschiedene Elemente aus k, sei $f_i = \prod_{j \neq i}(X - a_j)$. Dann ist $V(f_i) = \{a_1, \dots, a_{i-1}, a_{i+1}, \dots a_m\}$, also ist $V(f_1, \dots, f_m) = \emptyset$, während für jede echte Teilmenge $P' \subset P = \{f_1, \dots, f_m)$ gilt: $V(P')$ ist nicht leer.

Allerdings könnten wir ja die folgende schwächere Formulierung betrachten: *Zu jeder Menge $P \subseteq k[X_1, \dots, X_n]$ gibt es eine* **endliche** *Menge $P' \subset k[X_1, \dots, X_n]$ mit $V(P) = V(P')$.* Unser obiges Beispiel ist dann hinfällig: im Fall $n = 1$ arbeitet man mit einem Hauptidealring, also gilt: *Zu jeder Menge $P \subseteq k[X]$ gibt es ein Element $f \in k[X]$ mit $V(P) = V(f)$,* hier genügt es also, **einelementige** Mengen zu betrachten. Aber der Fall $n = 1$ ist uninteressant. Fall $n = 2$. Ist k ein unendlicher Körper, so kann man höchstens erwarten, daß es zu jeder Teilmenge $P \subseteq k[X_1, X_2]$ eine **zweielementige** Menge $P' \subset k[X_1, X_2]$ mit $V(P) = V(P')$ gibt: Nullstellenmenge eines einzigen Polynoms über einem unendlichen Körper sind immer unendliche Mengen! Die Dimensionstheorie wird uns zeigen, daß ganz allgemein gilt: *Nullstellenmengen von $n-1$ Polynomen in n Variablen über einem unendlichen Körper sind unendlich.*

Zariski-Topologie auf $X = \mathcal{V}(I)$. Eine Teilmenge $X' \subseteq X$ heißt *(Zariski-) abgeschlossen*, falls es ein Ideal $I' \supseteq I$ mit $X' = \mathcal{V}(I')$ gibt. Jede abgeschlossene Teilmenge ist also selbst wieder eine algebraische Menge. Es gilt:

(a) Durchschnitte abgeschlossener Mengen sind abgeschlossen.
(b) Die Vereinigung zweier abgeschlossener Mengen ist abgeschlossen.
(c) Die leere Menge wie auch X selbst sind abgeschlossen.

Insgesamt sehen wir: wir erhalten auf X eine "Topologie". Insbesondere können wir jeder Teilmenge $U \subseteq X$ ihren Abschluß $\overline{U}$ zuordnen; es ist $\overline{U}$ die kleinste abgeschlossenen Obermenge von U (also der Durchschnitt aller abgeschlossenen Teilmengen, die U enthalten ...). Die Komplemente abgeschlossener Mengen heißen offen (sie sind also durch Ungleichungen definiert).

Warnung: diese Topologie hat (verglichen mit der üblichen Topologie etwa des $\mathbb{R}^n$, des $\mathbb{C}^n$ oder auch der Funktionenräume in der Analysis) ganz merkwürdige Eigenschaften.

Beispiel: Der Abschluß einer unendlichen Teilmenge von $X = k$ ist immer X, für $k = \mathbb{R}$ oder $k = \mathbb{C}$ ist also $\overline{\mathbb{N}} = k$.

Es gilt (auch dies ist merkwürdig):

Folgerung aus dem Hilbert'schen Basissatz: *Sei $X \subseteq k^n$ eine algebraische Menge. Es gilt die absteigende Kettenbedingung für abgeschlossene Mengen in X.*

Wir nennen X irreduzibel, wenn sich X nicht als Vereinigung zweier echter abgeschlossener Teilmengen schreiben läßt. (Irreduzible algebraische Mengen nennt man oft “affine Varietäten”.)

Satz. *Jede algebraische Menge X läßt sich eindeutig als endliche Vereinigung paarweise unvergleichbarer irreduzibler abgeschlossener Mengen X_i schreiben.* Man nennt diese Teilmengen X_i die *irreduziblen Komponenten von X.*

Beweis: Aus dem Hilbert'schen Basissatz folgt unmittelbar, daß sich X als Vereinigung endlich vieler irreduzibler abgeschlossener Teilmengen schreiben läßt, etwa $X = \bigcup_{i=1}^n X_i$ mit paarweise unvergleichbaren abgeschlossenen Teilmengen X_i.

Sind $X, Y_1, \dots, Y_n$ algebraische Teilmengen von k^n und ist X irreduzibel, so folgt aus $X \subseteq \bigcup_{i=1}^n Y_i$, daß es ein i mit $X \subseteq Y_i$ gibt. Beweis mit Induktion nach n. Für $n = 1$ ist nichts zu zeigen. Sei also $n > 1$, setze $Y' = \bigcup_{i=1}^{n-1} Y_i$. Es ist $X \subseteq Y' \cup Y_n$, also $X = (Y' \cap X) \cup (Y_n \cap X)$. Da wir X als Vereinigung zweier abgeschlossener Mengen geschrieben haben, gilt $X = (Y' \cap X)$ oder $X = (Y_n \cap X)$. Im ersten Fall ist $X \subseteq Y'$ und wir können Induktion anwenden, im zweiten Fall ist $X \subseteq Y_n$.

Also sehen wir: *Sind $X_1, \dots, X_t$ die irreduziblen Komponenten der algebraischen Menge X, so ist die Vereinigung von $t-1$ dieser Teilmengen X_i eine echte Untermenge von X.*

Sei X eine algebraische Teilmenge von k^n.

Seien $X_1, \dots, X_n$ die irreduziblen Komponenten von X. Jede irreduzible abgeschlossene Teilmenge von X ist in einem X_i enthalten. Beweis: folgt aus der vorhergehenden Eigenschaft.

Eine irreduzible algebraische Menge $X' \subseteq X$ ist eine irreduzible Komponente von X, wenn es keine irreduzible algebraische Menge X'' mit $X' \subset X'' \subseteq X$ gibt. Beweis: Seien $X_1, \dots, X_n$ die irreduziblen Komponenten von X. Sei etwa $X_1 \subset X''$ mit X'' irreduzibel. Dann ist $X'' = \bigcup (X_i \cap X'')$, also $X'' = X_i \cap X''$ für ein i, also $X'' \subseteq X_i$ für dieses i, und demnach $X_1 \subset X'' \subseteq X_i$. Für $i = 1$ liefert die echte Inklusion einen Widerspruch, ansonsten verwendet man, daß die X_i paarweise unvergleichbar sind. Die Umkehrung folgt aus der vorhergehenden Eigenschaft: Ist X' eine irreduzible Teilmenge von X, so ist X' in einer irreduziblen Komponente von X enthalten.

Über einem algebraisch abgeschlossenen Körper gilt: *Sei $V \subseteq k^n$ eine algebraische Menge. Genau dann ist V irreduzibel, wenn $I(V)$ ein Primideal ist.*

Beweis: Zuerst nehmen wir an, daß $I(V)$ kein Primideal ist. Seien $f_1, f_2 \in mit f_1 f_2 \in I(V)$. Ist f_i nicht in $I(V)$, so ist $V_i = V(I(V) + Af_i)$ eine echte Teilmenge von V, und natürlich eine algebraische Menge. Wegen $f_1 f_2 \in U(V)$ ist $V_1 \cup V_2 = V$ (denn ist $v \in V$, so ist $f_1(v) f_2(v) = (f_1 f_2)(v) = 0$, also $f_1(v) = 0$ oder $f_2(v) = 0$). Dies zeigt, daß V nicht irreduzibel sein kann.

Sei nun V nicht irreduzibel, also $V = V_1 \cup V_2$ mit algebraischen Teilmengen V_i, die echt in V enthalten sind. Sei etwa $w_i \in V \setminus V_i$. Da V_i algebraische Teilmenge ist, gibt es ein $f_i \in I(V_i)$ mit $f_i(w_i) \neq 0$. Insbesondere gehört weder f_1 noch f_2 zu $I(V)$. Wegen $V = V_1 \cup V_2$ ist $(f_1 f_2)(v) = 0$ für alle $v \in V$, also $f_1 f_2$ gehört zu $I(V)$. Wir sehen, daß $I(V)$ kein Primideal sein kann.

C. Urbilder maximaler Ideale.

Sei $f\colon A \to B$ ein Ring-Homomorphismus. Dann gilt: Ist P ein Primideal von B, so ist $f^{-1}(P)$ ein Primideal von A. Insbesondere gilt also: Urbilder maximaler Ideale sind zumindest Primideale. Der Fall der Inklusionabbildung $\iota\colon \mathbb{Z} \to \mathbb{Q}$ und des maximalen Ideals 0 in $\mathbb{Q}$ (oder allgemeiner: Sei R ein Integritätsbereich, der kein Körper ist und $\iota\colon R \to \mathrm{Quot}(R)$ die Einbettung in den Quoteinetenkörper) zeigt, daß das Urbild eines maximalen Ideals kein maximales Ideal sein muß. Ist aber B eine affine k-Algebra mit k algebraisch abgeschlossen, und $f\colon A \to B$ ein k-Algebren-Homomorphismus, so ist das Urbild eines jeden maximalen Ideals wieder ein maximales Ideal. (Denn die maximalen Ideale von A sind Auswertungsideale, und das Urbild eines Auswertungsideals ist offensichtlich ein Auswertungsideal — unter f erhalten wir eine Inklusionsabbildung $A/f^{-1}(P) \subseteq B/P$, also ist immer $A/f^{-1}(P)$ ein Unterring eines Körpers; ist dieser Körper der Grundkörper k, so haben wir die Inklusionskette $k \subseteq A/f^{-1}(P) \subseteq B/P = k$.)

Wir sehen: Jeder k-Algebren-Homomorphismus $f\colon A \to B$ endlich erzeugter k-Algebren induziert eine Abbildung $f^*\colon \max B \to \max A$.

Mehrere Fälle sind zu betrachten:

- f ist surjektiv.
- f ist Inklusion und B ist ganz über A. Sei etwa B als Modul von m Elementen über A erzeugt. Dann gilt: Das Urbild eines jeden maximalen Ideals besteht aus höchstens m maximalen Idealen.

D. Maximale Primidealketten mit verschiedenen Längen.

Ein weiteres Beispiel: Sei $R = \mathbb{Z}_{(2)}$ die Menge der rationalen Zahlen, deren Nenner nicht durch 2 teilbar ist, und bilde $R[T]$. Das Ideal, das von $2T = 1$ erzeugt wird ist maximales Ideal (denn der Faktorring ist $\mathbb{Q}$) und als Hauptideal auch ein minimales Primideal. Andererseits gibt es die Idealkette

$$(0) \subset \langle T \rangle \subset \langle 2, T \rangle$$

von Primidealen.

E. “Going down”.

Satz. *Sei S Integritätsbereich, sei $R \subseteq S$ ein Unterring. Wir setzen voraus, daß R faktoriell ist und daß S endlich über R ist. Seien $P_0 \subset P_1$ Primideale von R. Ist Q_1 ein Primideal in S mit $Q_1 \cap R = P_1$, so gibt es ein Primideal Q_0 in S mit $Q_0 \subset Q_1$ und $Q_0 \cap R = P_0$.*

Beweis: Wir setzen zuerst nur voraus, daß $R \subseteq S$ eine endliche Erweiterung kommutativer Ringe ist.

(1) *Sei I ein Ideal in R. Ist $y \in IS$, so gibt es ein Polynom $f(X) = X^n + \sum_{i=0}^{n-1} r_i X^i$ mit Koeffizienten $r_i \in I$ für $0 \leq i < n$ und $f(y) = 0$.*

Beweis wie der von Lemma 1 im Abschnitt 1: Sei $S = \sum_i Rs_i$ mit Elementen $s_i \in S$ und $s_1 = 1$. Da ys_i zu $IS = \sum_i Is_i$ gehört, hat das dort konstruierte normierte Polynom die gewünschten Eigenschaften.

Sei nun zusätzlich S ein Integritätsbereich, sei R faktoriell mit Quotientenkörper K, und sei P ein Primideal in R.

(2) *Ist $y \in PS$ und ist $g(X) = X^n + \sum_{i=0}^{n-1} c_i X^i$ das Minimalpolynom von y über K, so gehören alle Koeffizienten c_i von $g(X)$ mit $0 \leq i \leq n-1$ zu P.*

Beweis: Sei $f(X)$ zu $P = I$ wie in (1) konstruiert. Da $g(X)$ das Minimalpolynom von y über K ist, gibt es ein Polynom $h(X) = X^m + \sum_{j=0}^{m-1} c'_j X^j$ mit Koeffizienten c'_j in K, so daß gilt $f(X) = g(X)h(X)$. Das Gauß-Lemma besagt, daß alle Koeffizienten c_i, c'_j von $g(X)$ und $h(X)$ zu R gehören. Die entsprechende Argumentation wie beim Beweis vom Gauß-Lemma zeigt, daß die Koeffizienten r'_i mit $0 \leq i \leq n-1$ sogar zu zu P gehören: Um dies zu zeigen, nehmen wir an, daß es $0 \leq a < n$ gibt mit $c_a \notin P$ und wir wählen das minimale derartige a. Wir setzen $c'_m = 1$, und wählen $0 \leq b \leq m$ minimal, so daß gilt $c'_b \notin P$ (wegen $c'_m = 1 \notin P$ gibt es derartige Koeffizienten). Der Koeffizient von $f(X)$ mit Index $a+b$ ist

$$\left(c_0 c'_{a+b} + \cdots + c_{a-1} c'_{b+1}\right) + c_a c'_b + \left(c_{a+1} c'_{b-1} + \cdots + c_{a+b} c'_0\right).$$

Wegen $a + b < n + m$ gehört dieser Koeffizient zu P. Die beiden Klammern sind jeweils Elemente von P, wegen der Minimalität von a, beziwhungsweise b. Also ist auch $c_a c'_b \in P$. Da P Primideal ist, muß dann aber auch einer der beiden Faktoren zu P gehören, ein Widerspruch. Also sehen wir, daß $g(X)$ die gewünschte Eigenschaft hat.

(3) *Sei P_0 ein Primideal von R, sei Q_1 ein Primideal von S, sei $P_0 \subseteq Q_1$. Dann gilt*

$$P_0 S (S \setminus Q_1)^{-1} \cap R = P_0.$$

(Wir betrachten hier Teilmengen des Quotientenkörpers L von S.)

Beweis: Sei $y \in P_0 S$, sei $s \in S \setminus Q_1$, sei $z = ys^{-1} \in R$. Angenommen z gehört nicht zu P_0. Sei $g(X) = X^n + \sum_{i=0}^{n-1} c_i X^i$ das normierte Minimalpolynom von y über K. Wegen (2) wissen wir, daß die Koeffizienten c_i zu P_0 gehören. Es ist $s = yz^{-1}$, und $0 \neq z^{-1} \in K$, also hat das Minimalpolynom von s ebenfalls Grad n. Multiplizieren wir

$$0 = g(y) = y^n + \sum_{i=0}^{n-1} c_i y^i$$

mit z^{-n}, so erhalten wir

$$0 = (yz^{-1})^n + \sum_{i=0}^{n-1} c_i z^{-n+i} (yz^{-1})^i,$$

demnach ist $X^n + \sum_{i=0}^{n-1} d_i X^i$ mit $d_i = c_i z^{-n+i}$ das Minimalpolynom von s über K. Da s ganz über R und R faktoriell ist, gehören alle diese Koeffizienten d_i zu R. Es ist $c_i = d_i z^{n-i}$. Da wir annehmen, daß z nicht zu P_0 gehört, und da $c_i \in P_0$, sehen wir: es ist $d_i \in P_0$ für $0 \leq i < n$. Also ist $s^n \in P_0 S \subseteq Q_1$, also $s \in Q_1$, ein Widerspruch.

(4) Nun also der Beweis des Satzes: Beachte: $S' = S(S \setminus Q_1)^{-1}$ ist ein Unterring des Quotientenkörpers L von S, und es ist $R \subseteq S \subseteq S' \subseteq L$. Die Menge $P_0 S(S \setminus Q_1)^{-1}$ ist ein Ideal in diesem Ring S'. Wir sehen also, daß es in S' Ideale I gibt mit $I \cap R = P_0$. Sei I ein Ideal von S', das maximal ist mit $I \cap R = P_0$. Ein derartiges Ideal ist maximal mit der Eigenschaft $I \cap (R \setminus P_0) = \emptyset$, also ist es (nach dem Primideallemma) ein Primideal. Wir haben $R \subseteq S \subseteq S'$. Setzen wir $Q_0 = I \cap S$, so ist auch Q_0 ein Primideal (Lemma 0 im Abschnitt 5), und es gilt $Q_0 \cap R = P_0$. Es bleibt zu zeigen, daß $Q_0 \subseteq Q_1$ gilt. Angenommen, es gibt $s \in Q_0 \setminus Q_1$. In S' ist s invertierbar, also ist $1 = ss^{-1}$ ein Element im Ideal I des Rings S'. Als Primideal ist aber I ein echtes Ideal.

F. Der Satz von Bézout.

Zwei Kurven in der Ebene vom Grad m und n schneiden sich "im allgemeinen" in mn Punkten. Dies ist der Satz von Bézout. Natürlich brauchen wir dazu einen algebraisch abgeschlossenen Grundkörper und die Kurven dürfen keine gemeinsame Komponente besitzen. Auch können Schnittpunkte uneigentliche Punkte sein (also unendlich ferne Punkte) und es können Schnitt-Multiplizitäten auftreten. Gutes Beispiel: zwei Ellipsen, die sich in vier Punkten schneiden .... Bewiesen wurde der Satz von Bézout 1779, vorher schon von Euler 1748, von Cramer 1750. Die genaue Formulierung lautet: F, G Kurven vom Grad m bzw n, ohne gemeinsame Komponente, sei $I_p(F,G)$ die "Schnitt-Multiplizität" von F und G im Punkt $p \in \mathbb{P}_2(k)$. Dann ist

$$\sum\nolimits_p I_p(F,G) = mn.$$

Dabei ist $I_p(F,G) \geq 0$ und $I_p(F,G) \geq 1$ genau dann, wenn gilt $p \in \mathcal{V}(F,G)$. Wir wollen das algebraische Substrat vorstellen, also konzentrieren wir uns auf Kurven, die keine uneigentliche Schnittpunkte besitzen. Woher kommen uneigentliche Schnittpunkte?

Ein Polynom $f \in k[X_1,\dots,X_n]$ heißt *homogen vom Grad d*, falls es eine Linearkombination von Monomen $\prod X_i^{d_i}$ mit $\sum_i d_i = d$ ist. Sei $k[X_1,\dots,X_n]_d$ der k-Vektorraum aller homogenen Polynome vom Grad d; seine Dimension ist $\binom{d+n-1}{d}$. Also zum Beispiel für $n=3$ gilt $\dim_k k[X,Y,Z]_d = \binom{d+2}{d} = \binom{d+2}{2} = \frac{1}{2}(d+2)(d+1)$ (denn es gibt $d-i+1$ Monome der Form $X^iY^jZ^{d-i-j}$, da $0 \leq j \leq d-i$ gelten muss; insgesamt sind dies $(d+1)+d+\cdots+2+1$ Monome).

Jedes Polynom $f \in k[X_1,\dots,X_n]$ läßt sich (eindeutig) als Summe $f = \sum_d f_d$ von homogenen Polynomen mit paarweise verschiedenen Graden schreiben. Ist $f = \sum_{d=0}^n f_d$ und $f_n \neq 0$, so nennt man n den *(Total-)Grad* von f.

Satz von Bézout. *Sei $f \in k[X,Y]$ ein Polynom vom Grad m und $g \in k[X,Y]$ ein Polynom von Grad n. Die Polynome f, g seien teilerfremd. Dann ist $\dim_k k[X,Y]/\langle f,g\rangle \leq mn$. Sind auch die Polynome f_m und g_n teilerfremd, so gilt Gleichheit.*

Bemerkung: Sind die Polynome f, g nicht teilerfremd, ist etwa h ein gemeinsamer nicht-konstanter Teiler, so ist $\langle f,g\rangle \subseteq \langle h\rangle$ und $k[X,Y]/\langle h\rangle$ ist unendlich-dimensional, also ist auch $k[X,Y]/\langle f,g\rangle$ unendlich-dimensional. Auch bezüglich der zweiten Behauptung gilt die Umkehrung (dies ist nicht ganz so offensichtlich); hier wenigstens ein Beispiel, das zeigt, wie wichtig die zweite Teilerfremdheits-Bedingung ist: Es ist $\langle X, XY-1\rangle = k[X,Y]$.

Beweis: Jedem Polynom $f \in k[X,Y]$ mit $f = \sum_{d=0}^n f_d$ und $f_n \neq 0$ ordnen wir das homogene Polynom $f^* = \sum_{d=0}^n f_d Z^{n-d} \in k[X,Y,Z]$ zu, es hat den Grad n. Ist umgekehrt $F \in k[X,Y,Z]$ homogen vom Grad n, so bilde $F_*(X,Y) = F(X,Y,1)$, dies ist ein Polynom vom Grad höchstens n und es gilt

$$(f^*)_* = f \quad \text{und} \quad (F_*)^* Z^r = F$$

für ein r mit $0 \leq r \leq n$.

Sei $R = k[X,Y,Z]$, sei $F = f^*, G = g^*$ und $d \geq m+n$. Sei U_d der Unterraum von R_d aller Formen vom Grad d der Form $AF + BG$ (mit $A \in R_{d-m}$ und $B \in R_{d-n}$). Wir zeigen: *Es ist* $\dim R_d/U_d = mn$.

Beweis: Es gibt eine exakte Folge

$$0 \to R_{d-m-n} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\phi} R_d \to R_d/U_d \to 0,$$

dabei ist $\psi(C) = (CF, -CG)$ und $\phi(A,B) = AF + BG$. Klar ist, daß ψ injektiv ist, denn R ist nullteilerfrei. Offensichtlich ist $\phi\psi = 0$. Umgekehrt sieht man: ist das Paar (A,B) im Kern von ϕ, also $AF + BG = 0$, so ist F, aber auch G ein Teiler von $AF = -BG$. Da f, g teilerfremd sind, sind auch F, G teilerfremd. Demnach ist FG ein Teiler von AF, also $CFG = AF = -BG$ und demnach $CG = F$ und $CG = -B$, also ist $(A,B) = \psi(C)$. Aus der Formel $\dim_k R_d = \binom{d+2}{2}$ folgt $\dim_k R_d/U_d = mn$.

Sei nun $A_1, \ldots, A_{mn}$ eine Komplementärbasis von U_d in R_d (die Restklassen modulo U_d bilden also eine Basis von R_d/U_d. *Sei* $h \in k[X,Y]$ *ein Polynom vom Grad höchstens* d. *Wir zeigen, daß sich* h *modulo* $\langle f, g\rangle$ *als Linearkombination der Polynome* $a_i = (A_i)_*$ *schreiben läßt.* (Demnach ist dann $\dim_k k[X,Y]/\langle f,g\rangle \leq mn$.) Denn sei r der Grad von h, also hat h^*Z^{d-r} den Grad d, gehört also zu R_d. Also gibt es $\lambda_i \in k$ und B, C Formen mit

$$h^*Z^{d-r} = \sum\nolimits_{i=1}^{mn} \lambda_i A_i + BF + CG.$$

Wende $_*$ an, wir erhalten

$$h = \sum\nolimits_{i=1}^{mn} \lambda_i (A_i)_* + B_* f + C_* g.$$

Seien nun auch die Polynome f_m, g_n teilerfremd. Was sind dies für Polynome? Es ist $f_m = f^*(X,Y,0)$ und $g_n = g^*(X,Y,0)$. Wir zeigen: *Die Multiplikation mit* $\overline{Z}$ *liefert einen injektiven Vektorraum-Endomorphismus von* $R/\langle F, G\rangle$*, also eine injektive Abbildung* $R_d/U_d \to R_{d+1}/U_{d+1}$.

Beweis: Sei also $H \in R_d$ und $ZH = AF + BG$ mit A, B homogen. Ist $J \in k[X,Y,Z]$, so setze $J_0 = J(X,Y,0) \in k[X,Y]$. Insbesondere ist $f_m = F_0$, und $g_n = G_0$. Beachte: Genau dann ist $J_0 = 0$, wenn Z ein Teiler von J ist.

Aus $ZH = AF + BG$ folgt $0 = A_0F_0 + B_0G_0$. Nun sind F_0, G_0 teilerfremde Teiler von A_0F_0, also ist F_0G_0 Teiler von A_0F_0, etwa $F_0G_0C = A_0F_0 = -B_0G_0$. Also $G_0C = A_0$ und $F_0C = -B_0$. Aus $(A - GC)_0 = 0$ folgt, daß Z ein Teiler von $A - GC$ ist, etwa $ZA' = A - GC$. Aus $(B + FC)_0 = 0$ folgt, daß Z ein Teiler von $B + FC$ ist, etwa $ZB' = B + FC$. Demnach ist $ZA'F + ZB'G = (A - GC)F + (B + FC)G = AF + BG = ZH$ und also $A'F + B'G = H$.

Wähle $d = m + n$ und eine Komplementärbasis $A_1, \ldots, A_{mn}$ von U_d in R_d. Wir zeigen, daß die Elemente $a_i = (A_i)_*$ in $k[X,Y]/\langle f, g\rangle$ linear unabhängig sind. Sei etwa

$$\sum\nolimits_i \lambda_i (A_i)_* = bf + cg$$

mit $b, c \in k[X,Y]$. Dann gibt es natürliche Zahlen r, s, t mit

$$Z^r \sum\nolimits_i \lambda_i A_i = Z^s b^* F + Z^t c^* G$$

Also gilt in R_{d+r}/U_{d+r} die Relation $\sum_i \lambda_i \overline{Z^r A_i} = 0$. Da nun die Elemente $Z^r A_i$ in R_{d+r}/U_{d+r} linear unabhängig sind, folgt $\lambda_i = 0$ für alle i.

Wir haben gebraucht: Seien $f, g \in k[X, Y]$, sei t der Grad von f und s der Grad von g. Dann gilt:

- $(fg)^* = f^* g^*$.
- $Z^r(f+g)^* = Z^s f^* + Z^t g^*$ mit $r = s + t - \deg(f+g)$.

Seien f, g nicht-konstante Polynome in zwei Variablen. Sei $p \in \mathbb{A}^2$. Setze

$$I_p(f, g) = \dim \mathcal{O}_p(\mathbb{A}^2)/\langle f, g\rangle,$$

wir nennen dies die Schnittzahl von f und g im Punkt p.

(1) *Haben f, g einen nicht-konstanten Faktor h und ist $p \in \mathcal{V}(h)$, so ist $I_p(f, g) = \infty$, andernfalls ist $I_p(f, g) \in \mathbb{N}_0$. Es ist $I_p(f, g) \geq 1$ genau dann, wenn $p \in \mathcal{V}(f, g)$.*

Proposition. *Sei k ein algebraisch abgeschlossener Körper und sei I ein co-endliches Ideal in $k[T_1, \ldots, T_n]$. Seien $p_1, \ldots, p_t$ paarweise verschiedene Punkte in $\mathbb{A}^n$ mit $\mathcal{V}(I) = \{p_1, \ldots, p_n\}$. Dann ist die kanonische Abbildung*

$$\phi\colon\ k[T_1, \ldots, T_n]/I \to \prod\nolimits_i \mathcal{O}_i/\mathcal{O}_i I$$

mit $\phi(f+I)_i = f + \mathcal{O}_i I$ ein Algebren-Isomorphismus. (Natürlich schreibt man üblicherweise $\overline{f}$ statt $f + I$ oder $f + \mathcal{O}_i I$, um die Restklasse von f im Faktorring zu notieren; zur Verdeutlichung haben wir hier die umständlichere Notation verwandt.)

Beweis: Übungsaufgabe.

Wir brauchen:

Lemma. *(Sei k algebraisch abgeschlossen.) Sei $f \in k[X, Y]$. Sei $p \in \mathcal{V}(f)$. Die folgenden Eigenschaften sind äquivalent:*
(1) $(f_x(p), f_y(p)) \neq (0, 0)$.
(2) *$\mathcal{O}_p(\mathbb{A}^2)/\langle f\rangle$ ist diskreter Bewertungsring.*

In diesem Fall heißt p ein *einfacher* Punkt von f; ist $f_x(p) \neq 0$, so wird das maximale Ideal von $\mathcal{O}_p(\mathbb{A}^2)/\langle f\rangle$ von der Restklasse von Y erzeugt (sonst von der Restklasse von X).

Definition: Jede Funktion $u \in \mathcal{O}_p$, die das maximale Ideal von $\mathcal{O}_p$ erzeugt, heißt *Orts-Uniformisierende im Punkt p.*

Beweis: Sei $p = (p_1, p_2)$. Sei $\mathcal{O} = \mathcal{O}_p(\mathbb{A}^2)$. Sei $\mathbf{m}$ das maximale Ideal von $\mathcal{O}$, es wird von $X - p_1, Y - p_2$ erzeugt.

(1) $\implies$ (2). Wir setzen obdA voraus $f_x(p) \neq 0$. Es ist $f = (X - p_1) cdot a + (Y - p_2) \cdot b$, mit $a, b \in k[X, Y]$. Ableitung nach X liefert $f_x = a + (X - p_1) a_x + (Y - p_2) b_x$, also $0 \neq f_x(p) = a(p)$. Also können wir in $\mathcal{O}$ durch a teilen und erhalten $X - p_1 = f \cdot a^{-1} + (Y - p_2) \cdot b \cdot a^{-1}$. Modulo f ist also $X - p_1$ ein Vielfaches von $Y - p_2$.

Umgekehrt sei (2) erfüllt. Da $\mathbf{m}/\langle f\rangle$ von einem Element erzeugt wird, nehmen wir oBdA an, daß es von $Y-p_2$ erzeugt wird, also wird $\mathbf{m}$ von f und $Y-p_2$ erzeugt, es ist also $X-p_1 = uf + v(Y-p_2)$, mit $u,v \in \mathcal{O}$. Es gibt $s \in k[X,Y]$ mit $s(p) \neq 0$ und $su, sv \in k[X,Y]$, also $s(X-p_1) = (su)f + (sv)(Y-p_2)$. Ableitung nach X liefert $s_x(X-p_1) + s = (su)_x f + (su)f_x + (sv)_x(Y-p_2)$. Auswertung an der Stelle p ist $s(p) = (su)(p)f_x(p)$, also ist $f_x(p) \neq 0$.

Bemerkung. Schreibe $f = \sum_{i=s}^t f_i$, dabei sei f_i eine Form vom Grad i und $f_s \neq 0, f_t \neq 0$ und $s \leq t$. Trivialerweise gilt: *Es ist* $0 \in (f)$ *genau dann, wenn* $s \geq 1$.

Sei nun $f(0) = 0$. *Ist* $f_1 = aX + bY$, *so ist* $(f_x(0), f_y(0)) = (a,b)$. Ist nämlich $f = X^iY^j$, so ist sowohl $f_x = iX^{i-1}Y^j$ als auch f_y Vielfaches eines Monoms vom Grad $i+j-1$, also gilt $(f_x(0), f_y(0)) = (0,0)$ für $i+j > 1$; entsprechendes gilt für Linearkombinationen von Monomen. Ist umgekehrt $f_1 \neq 0$, also $f_1 = aX + bY$, so ist $f_x = a$ und $f_y = b$.

Also: *Genau dann ist also* $(f_x(0), f_y(0)) \neq 0$, *wenn* $f_1 \neq 0$ *gilt.*

Also: *Genau dann ist* $0 \in \mathcal{V}(f)$ *ein einfacher Punkt, wenn* $s = 1$.

Allgemeiner betrachten wir nun s minimal mit $f_s \neq 0$. Wir schreiben diese Form als Produkt von Linearfaktoren L_j und erhalten damit die *Tangenten* an f im Punkt 0 (dies sind also endlich viele Geraden mit gewissen Vielfachheiten.) Sind alle Vielfachheiten 1 (oder 0), so nennt man 0 einen *gewöhnlichen Mehrfachpunkt.* Man nennt s die *Multiplizität* $m_0(f)$ *von* f *im Punkt* 0 und f_s den zugehörigen Führungsterm.

Durch einen affinen Koordinatenwechsel kann man erreichen, daß ein vorgegebener Punkt p in den Ursprung verschoben wird; deshalb setzen wir jetzt $p = 0$ voraus, denn dies entspricht der üblichen Basiswahl in $k[X,Y]$: man arbeitet mit Monomen X^iY^j. Genauso gut könnte man als Basis die Polynome $(X-a)^i(Y-b)^i$ nehmen; dann würde man direkt an der Stelle $p = (a,b)$ arbeiten. Auf diese Weise erhält man die *Multiplizität* $m_p(f)$ *von* f *im Punkt* p.

Fundamentalsatz von Max Noether. *Seien* F, G, H *Formen in* $k[X,Y,Z]$. *Wir setzen voraus, daß die Formen* F, G *keine gemeinsame Komponente haben. und daß die gemeinsamen Punkte von* F *und* G *einfache Punkte von* F *sind. Gilt dann*

$$I_p(F,G) \leq I_p(F,H) \quad \textit{für alle} \quad p \in \mathbb{P}_2,$$

so gibt es eine Form B *mit*

$$I_p(F,G) + I_p(F,B) = I_p(F,H) \quad \text{für alle} \quad p \in \mathbb{P}_2.$$

Zusatz: Der Beweis zeigt: es ist $H \in \langle F, G\rangle$, und zwar gibt es Formen A, B mit $H = AF + BG$. Wir nehmen nun ein solches B. Beachte: Schreiben wir $H = uF + vG$ mit Polynomen u, v und schreiben wir $u = \sum U_i, v = \sum V_i$ mit Formen U_i, V_i vom Grad i, so folgt aus $H = \sum U_iF + \sum V_iG$, daß gilt $H = U_rF + V_sG$ mit $r = \operatorname{grad} H - \operatorname{grad} F$ und $s = \operatorname{grad} H - \operatorname{grad} G$.

Beweis: Wir können voraussetzen, daß alle Schnittpunkte von F und G im Endlichen liegen und betrachten wieder $f = F_*, g = G_*$ und auch $h = H_* =$

$H(X,Y,1)$. Das folgende Lemma zeigt, daß $h \in \mathcal{O}_p\langle f,g\rangle$ liegt. Der chinesische Restsatz zeigt: $h \in k[X,Y]/\langle f,g\rangle$, also gilt $H_* = aF_* + bG_*$ mit $a,b \in k[X,Y]$ und demnach $Z^r H = A'F + B'G$ mit Formen A', B' (die notwendigen Faktoren Z sind in A' und B' eingearbeitet). Die Multiplikation mit Z ist auf $k[X,Y,Z]/\langle F,G\rangle$ injektiv, also ist $H \in \langle F,G\rangle$, etwa $H = AF + BG$.

Es ist $I_p(F,H) = I_p(F, AF+BG) = I_p(F,BG) = I_p(F,B) + I_p(F,G)$ (dabei verwenden wir zwei wichtige Eigenschaften der Schnittzahlen).

Ist p ein einfacher Punkt von f, und $I_p(f,g) \le I_p(f,h)$, so ist $h \in \mathcal{O}_p\langle f,g\rangle$.

Beweis: Betrachte den diskreten Bewertungsring $\mathcal{O}/\langle f\rangle$ und die beiden Ideale $\langle f,g\rangle/\langle f\rangle$ (mit Codimension $I_p(f,g)$) und $\langle f,h\rangle/\langle f\rangle$ (mit Codimension $I_p(f,h)$). Da in einem diskreten Bewertungsring je zwei Ideale vergleichbar sind, gilt hier $\langle f,h\rangle/\langle f\rangle \subseteq \langle f,g\rangle/\langle f\rangle$, also $h \in \langle f,g\rangle$.

Folgerungen: Satz von Pappos, von Pascal.

Teil II. Anfänge der Modul-Theorie.

Sei R ein Ring.

Moduln. Ein R-Linksmodul M (oder einfach ein Modul) ist eine abelsche Gruppe zusammen mit einer bilinearen Abbildung $\mu\colon R \times M \to M$, so dass für alle $m \in M$ und alle $r, r' \in R$ gilt:
(1) $\mu(1, m) = m$,
(2) $\mu(r, \mu(r', m)) = \mu(rr', m)$.
Statt $\mu(r, m)$ schreibt man meist einfach rm, die Eigenschaft (2) schreibt sich dann als "Assoziativgesetz" $r(r'm) = (rr')m$. Manchmal schreibt man ${}_RM$ statt M, um auf R zu verweisen.

Beispiel 1: *Ist $R = k$ ein Körper, so sind R-Linksmoduln nichts anderes als k-Vektorräume.*

Beispiel 2: *Jeder Ring R kann auch als R-Linksmodul aufgefaßt werden, man schreibt dann lieber ${}_RR$.*

Untermoduln. Ist M ein Modul, so nennt man eine Teilmenge $U \subseteq M$ einen *Untermodul,* falls U eine Untergruppe von M ist und für alle $r \in R, m \in U$ gilt: $rm \in U$.

Beispiel: *Die Untermoduln von ${}_RR$ sind gerade die Linksideale.*

Faktormoduln. Ist $U \subseteq M$ ein Untermodul des Moduls M, so ist die Faktorgruppe M/U in kanonischer Weise wieder ein R-Modul (durch $r\overline{m} = \overline{rm}$), man nennt ihn den zugehörigen Faktormodul.

Homomorphismen. Sind M, N Moduln (also R-Linksmodul für einen festgewählten Ring R), so ist ein Homomorphismus (genauer ein R-Homomorphismus) $f\colon M \to N$ eine additive Abbildung (es ist also $f(m_1 + m_2) = f(m_1) + f(m_2)$ für alle $m_1, m_2 \in M$), für die zusätzlich gilt $f(rm) = rf(m)$ für alle $r \in R, m \in M$.

Triviale Beispiele: Ist $U \subseteq M$ ein Untermodul, so ist die Inklusionsabbildung $U \to M$ mit $u \mapsto u$ ein Homomorphismus, entsprechend ist $M \to M/U$ mit $m \mapsto \overline{m}$ ein Homomorphismus (die sogenannte *Projektionsabbildung*).

Einen injektiven Homomorphismus nennt man *Monomorphismus*, einen surjektiven Homomorphismus nennt man *Epimorphismus,* einen Homomorphismus, der sowohl injektiv als auch surjektiv ist, einen *Isomorphismus:* Ist nämlich f injektiver und surjektiver Homomorphismus, so ist auch f^{-1} ein Homomorphismus (zeigen!). Gibt es einen Isomorphismus $f\colon M \to N$, so nennt man M, N isomorph und man schreibt $M \simeq N$.

Ist $f\colon M \to N$ ein Homomorphismus von R-Linksmoduln, so nennt man $\operatorname{Ker} f = \{x \in M \mid f(x) = 0\}$ den *Kern* von f (und $f(M)$ das *Bild* von f). *Der Kern eines Homomorphismus $f\colon M \to N$ ist ein Untermodul von M, das Bild $f(M)$ ist ein Untermodul von N und f induziert einen Isomorphismus $\overline{f}\colon M/\operatorname{Ker} f \to f(M)$ (mit $\overline{f}(\overline{m}) = f(m)$).* (Erster Isomorphie-Satz).

Ein Homomorphismus $f\colon M \to N$ liefert eine Bijektion zwischen den Untermoduln von M, die $\operatorname{Ker} f$ *enthalten und den Untermoduln von $f(M)$; diese Bijektion ist ist inklusions-erhaltend und -reflektierend.* Beweis: Übungsaufgabe.

Sind Untermoduln $U \subseteq V \subseteq M$ gegeben, so ist V/U ein Untermodul von M/U und es gibt einen kanonischen Isomorphismus $(M/U)/(V/U) \simeq M/V$. Beweis: Übungsaufgabe.

Durchschnitte von Untermoduln sind wieder Untermoduln; Vereinigungen im algemeinen nicht. Sind U_i Untermoduln von M, so schreibt man $\sum_i U_i$ für die Menge aller endlichen Summen $\sum_i u_i$ mit $u_i \in U_i$, dies ist wieder ein Untermodul, die *Summe* der U_i, und zwar ist dies der kleinste Untermodul von M, der alle U_i enthält.

Erzeugendensysteme. Ist $x \in M$, so ist $Rx = \{rx \mid r \in R\}$ ein Untermodul, man nennt ihn den von x *erzeugten* Untermodul; gilt $M = Rx$ für ein $x \in M$, so nennt man M *zyklisch.* Sind $x_i \in M$ mit $i \in I$, so nennt man $\sum_i Rx_i$ den von den Elementen x_i *erzeugten* Untermodul; gibt es eine endliche Menge $x_1, \dots, x_n \in M$ mit $M = \sum_{i=1}^n Rx_i$, so nennt man M *endlich erzeugt.*

Beispiele von Moduln, die nicht endlich erzeugt sind: ${}_{\mathbb{Z}}\mathbb{Q}$ (hier gilt zusätzlich: Ist $(x_i)_{i \in I}$ ein Erzeugendensystem, und ist I' eine endliche Menge, so ist auch $(x_i)_{i \in I \setminus I'}$ ein Erzeugendensystem).

Interne direkte Summen. Sind U_i Untermoduln von M mit $i \in I$, dabei sei I eine Indexmenge, so nennt man M die *direkte Summe* der U_i und schreibt $M = \bigoplus_i U_i$, falls gilt: Sind Elemente $u_i \in U_i$ mit $\sum_i u_i = 0$ gegeben (dabei seien fast alle $u_i = 0$), so ist $u_i = 0$ für jedes i (man spricht auch von einer *direkten Zerlegung* von M). Ist $I = \{1, 2, \dots, n\}$, so schreibt man meist $M = U_1 \oplus U_2 \oplus \cdots \oplus M_n$. Ist U ein Untermodul von M, so nennt man U einen *direkten Summanden* von M, falls es einen Untermodul U' von M mit $M = U \oplus U'$ gibt.

Lemma. (Charakterisierung direkter Summanden). (a) Ein Untermodul $U \subseteq M$ ist genau dann ein direkter Summand, wenn es einen Homomorphismus $\pi\colon M \to U$ mit $\pi(u) = u$ für alle $u \in U$ gibt. (b) Sind Homomorphismus $\phi\colon M \to N$ und $\psi\colon N \to M$ mit $\psi \circ \phi = 1_M$ gegeben, so ist ϕ injektiv, ψ surjektiv, und es ist $N = \phi(M) \oplus \operatorname{Ker}(\psi)$; insbesondere ist also $\phi(M)$ ein direkter Summand von N.

Beispiel. Dies ist nicht einfach nur ein Beispiel, sondern eine **Fundamental-Einsicht,** die viele Anwendungen besitzt, und die als Ausgangsbeispiel für die Theorie der Dedekind-Ringe dient — gerade deswegen müssen wir uns an dieser Stelle mit Moduln beschäftigen!

Sei R ein Hauptidealbereich (R ist also ein Integritätsbereich und jedes Ideal ist ein Hauptideal). Dann ist R ein Ring mit eindeutiger Primfaktorzerlegung. Sei Q der Quotientenkörper von R.

Ist p ein Primelement, so erhalten wir eine Kette von zyklischen Untermoduln

$$R \subset R\tfrac{1}{p} \subset R\tfrac{1}{p^2} \subset R\tfrac{1}{p^3} \subset \cdots \subset \bigcup\nolimits_{n \in \mathbb{N}} R\tfrac{1}{p^n} = R[\tfrac{1}{p}],$$

dabei ist $R[\frac{1}{p}]$ die Menge aller Elemente der Form $\frac{a}{p^n}$ mit $a \in R$ und $n \in \mathbb{N}_0$, also der kleinste Unterring von Q, der R und $\frac{1}{p}$ enthält. Wir bilden nun die entsprechenden

Faktormoduln modulo R und erhalten entsprechend eine Kette von Untermoduln

$$0 = R/R \subset R\tfrac{1}{p}/R \subset R\tfrac{1}{p^2}/R \subset \cdots \subset \bigcup_{n\in\mathbb{N}_0} R\tfrac{1}{p^n}/R = R[\tfrac{1}{p}]/R;$$

man nennt $R[\frac{1}{p}]/R$ den Prüfer-Modul zu p, *dieser Prüfermodul besitzt keine weiteren Untermoduln.* (Beweis: es reicht zu zeigen, daß alle zyklischen Untermoduln in dieser Kette vorkommen. Betrachte den von der Restklasse von $\frac{a}{p^n}$ erzeugten Untermodul, dabei können wir voraussetzen, daß p kein Teiler von a ist. Einerseits ist $\frac{a}{p^n} = a\frac{1}{p^n}$, also ist $R\frac{a}{p^n} \subseteq R\frac{1}{p^n}$. Andererseits gibt es wegen $(p^n, a) = 1$ Elemente $r, s \in R$ mit $ra + sp^n = 1$, demnach ist $\frac{1}{p^n} = r\frac{a}{p^n} + s$, also ist die Restklasse von $\frac{1}{p^n}$ ein skalares Vierlfaches der Restklasse von $\frac{a}{p^n}$. Dies zeigt: Die Restklasse von $\frac{a}{p^n}$ erzeugt den Modul $R\frac{1}{p^n}/R$.

Sei nun P eine vollständiges Repräsentantensystem von Primelementen (P enthält also genau ein Element aus jeder Klasse assoziierter Elemente). Behauptung:

$$(*) \qquad Q/R = \bigoplus\nolimits_{p\in P} R[\tfrac{1}{p}]/R.$$

Beweis: Zweierlei ist zu zeigen. Erstens, dass gilt $Q = \sum R[\frac{1}{p}]$, daß sich also jedes Element aus Q als Summe von Elementen mit Primpotenznennern schreiben läßt. (Sind $b_1, b_2 \in R$ teilerfremd, so gibt es $r_1, r_2 \in R$ mit $1 = r_1b_1 + r_2b_2$, also ist $\frac{a}{b_1b_2} = \frac{ar_2}{b_1} + \frac{ar_1}{b_2}$. Mit Induktion folgt die Behauptung.) Man erhält also die Summendarstellung $Q/R = \sum R[\frac{1}{p}]/R$. Zweitens ist nun noch zu zeigen, daß dies eine direkte Summe ist, daß also gilt: Sind die Primelemente $p_1, \dots, p_t$ paarweise nicht-assoziiert, und gilt $\sum \frac{a_i}{p_i^n} \in R$, so ist p_i^n ein Teiler von a_i für jedes i, also $\frac{a_i}{p_i^n} \in R$ (nachrechnen).

Bemerkung: Wir nennen eine direkte Zerlegung $M = \bigoplus U_i$ *starr*, wenn jeder Untermodule von M die Form $\bigoplus U_i'$ mit Untermoduln $U_i \subseteq U_i$ hat. Üblicherweise sind direkte Zerlegungen nicht starr (schon das Beispiel des k-Moduls k^2 zeigt dies!) — hier dagegen gilt: *Die direkte Zerlegung $Q/R = \bigoplus_p R[\frac{1}{p}]/R$ eines Hauptidealbereichs ist starr.* Beweis: Übungsaufgabe. Da die Untermoduln jedes Prüfer-Moduls $R[\frac{1}{p}]/R$ durch $\mathbb{N}_0 \cup \{\infty\}$ beschrieben werden, werden demnach die Untermoduln von Q/R durch eine Funktion $P \to \mathbb{N}_0 \cup \{\infty\}$ beschrieben. entsprechend werden endlich-erzeugte Untermoduln von Q/R durch eine Funktion h: $P \to \mathbb{N}_0$ mit endlichem Träger beschrieben ("endlicher Träger" bedeutet, daß $h(p) = 0$ für fast alle $p \in P$ gilt).

Ist $R = \mathbb{Z}$, so liefert $(*)$ die direkte Zerlegung

$$\mathbb{Q} = \bigoplus_{p \text{ Primzahl}} \mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z},$$

die vieles über das Arbeiten mit Brüchen erklärt (und eigentlich auch zeigt, warum die übliche Bruchrechnung durchaus kompliziert ist).

Ist $R = k[T]$ der Polynomring in einer Variablen über einem Körper, so nennt man die durch $(*)$ gegebene Zerlegung

$$k(T) = \bigoplus_{f \text{ irred, normiert}} k[T, \tfrac{1}{f}]/k[T]$$

die *Partialbruch-Zerlegung* der rationalen Funktionen, sie spielt eine wichtige Rolle zum Beispiel beim Integrieren (hier ist $k = \mathbb{R}$ oder $\mathbb{C}$). Ist zum Beispiel k algebraisch abgeschlossener Körper, so ist die Indexmenge P die Menge der linearen normierten Polynome $T - \lambda$ (mit $\lambda \in k$) und es folgt: Die Polynome

$$T^n \quad \text{und} \quad \tfrac{1}{(T-\lambda)^n} \quad \text{mit} \quad n \in \mathbb{N}_1$$

bilden zusammen mit 1 eine k-Basis von $k(T)$.

Bevor wir dieses Beispiel verlassen, mache man sich noch einmal klar: wir beschreiben hier Q/R sehr detailliert. Was ist die algebraische Struktur von Q/R? Es ist **kein** Ring, natürlich ist Q/R eine abelsche Gruppe, aber Q/R besitzt (falls $R \neq \mathbb{Z}$) **mehr** Struktur, es ist nämlich ein R-Modul (mehr Struktur = weniger Untermoduln). Um Moduln wie Q/R analysieren zu können, haben wir den Modul-Begriff eingeführt. Wichtig ist der Begriff der direkten Zerlegung (und natürlich der eines Untermoduls): wir beschreiben Q/R als direkte Summe der Untermoduln $R[\frac{1}{p}]/R$. Zur Analyse dieser Moduln $R[\frac{1}{p}]/R$ brauchen wir wieder den Begriff des Untermoduls, und auch den eines zyklischen Moduls (wie wir gesehen haben, sind alle echten Untermoduln von $R[\frac{1}{p}]/R$ zyklisch). Man merke sich: ein solcher Prüfer-Modul ist nicht artinsch, d.h es gilt **nicht** die aufsteigende Kettenbedingung für Untermoduln.

Noch etwas: Wie sehen die endlich-erzeugten Untermoduln $U \neq 0$ von Q aus? Man sieht sofort: *Ist $U \subset Q$ endlich erzeugt, so ist U zyklisch* (Beweis: Übungsaufgabe). Sei also $q \in Q \setminus \{0\}$ und $U = Rq$. Wir schreiben $q = \epsilon \prod_{p \in P} p^{e(p)}$, dabei ist ϵ ein invertierbares Element von R und $e\colon P \to \mathbb{Z}$ eine Funktion mit endlichen Träger (ist $e'(p)$ der Exponent der höchstens Potenz von p, die a teilt, und $e''(p)$ der Exponent der höchstens Potenz von p, die b teilt, so ist $e(p) = e'(p) - e''(p)$. Dann sehen wir: wir erhalten auf diese Weise *eine Bijektion zwischen den endlich-erzeugten, von Null verschiedenen Untermoduln von Q und den Funktion $e\colon P \to \mathbb{Z}$ mit endlichem Träger.*

Externe direkte Summen. Sind Moduln M_i mit $i \in I$ gegeben, so bildet die Menge M der Funktionen $x\colon I \to \bigcup M_i$ mit $x(i) \in M_i$ und $x(i) = 0$ für fast alle i einen Modul bezüglich komponentenweiser Addition und komponentenweiser Skalarmultiplikation; man nennt M die *externe direkte Summe* der Moduln M_i (und man schreibt meist x_i statt $x(i)$). Für jedes $i \in I$ ist die Menge $M(i)$ der Elemente x mit $x_j = 0$ für $j \neq 0$ ein zu M_i (kanonisch) isomorpher Untermodul von M und es ist $M = \bigoplus_i M(i)$. es zeigt sich also: *Die externe direkte Summe der Moduln M_i ist die interne direkte Summe der Moduln $M(i)$ (und diese sind zu den Moduln M_i kanonisch isomorph).* Gilt $M_i = N$ für alle $i \in I$, so bezeichnet man mit $N^{(I)}$ die entsprechende externe direkte Summe; ist $I = \{1, 2, \dots, n\}$, so schreibt man N^n statt $M^{(I)}$.

Basen. Ein Erzeugendensystem x_i ($i \in I$) eines Moduls M heißt *Basis,* wenn gilt: Sind Elemente $r_i \in R$ gegeben, von denen fast alle Null sind, und gilt $\sum_i r_i x_i = 0$, so gilt $r_i = 0$ für alle i. In diesem Fall ist einerseits $M = \bigoplus_i Rx_i$ und andererseits sind die Moduln Rx_i und ${}_RR$ isomorph (unter der Abbildung ${}_RR \to Rx_i$ mit $r \mapsto rx_i$. Es ist also M isomorph zur externen direkten Summe von Kopien von ${}_RR$, mit Indexmenge I. Derartige Moduln nennt man *freie Moduln.*

Endlich-erzeugte Moduln, noethersche Moduln. *Ein Modul M ist genau dann endlich erzeugt, wenn es einen Epimorphismus $({}_RR)^n \to M$ gibt* (statt $({}_RR)^n$ schreibt man oft einfach R^n). Beweis: Übungsaufgabe.

Ist R linksnoetherscher Ring, so ist jeder Untermodul eines endlich-erzeugten Moduls endlich-erzeugt. Beweis: Übungsaufgabe.

Projektive Moduln. Sei R ein Ring und M ein R-Modul. Die folgenden Eigenschaften sind äquivalent:
(i) M ist isomorph zu einem direkten Summanden eines freien Moduls.
(ii) (Hochhebungs-Eigenschaft). Ist ϵ: $N_1 \to N_2$ ein Epimorphismus und ϕ_2: $M \to N_2$ ein Homomorphismus, so gibt es einen Homomorphismus ϕ_1: $M \to N_1$ mit $\phi_2 = \epsilon \circ \phi_1$.
(iii) (Retraktions-Eigenschaft). Ist ϵ: $N \to M$ ein Epimorphismus, so gibt es einen Homomorphismus σ: $M \to N$ mit $\epsilon \circ \sigma = 1_M$.
In diesem Fall nennt man M einen *projektiven* Modul. Projektive Moduln sind abgeschlossen unter direkten Summen und direkten Summanden.

Beweis: Übungsaufgabe.

Sei I ein Ideal des Integritätsbereichs R. Man sagt, daß I invertierbar ist, wenn es einen Untermodul $I' \subseteq \operatorname{Quot}(R)$ gibt mit $I \cdot I' = R$. Offensichtlich ist jedes von Null verschiedene Hauptideal invertierbar. Im Polynomring $R = k[X, Y]$ in zwei Variablen mit Koeffizienten in einem Körper k ist das von X, Y erzeugte Ideal $I = \langle X, Y\rangle$ **nicht** invertierbar.

Lemma. *Sei R ein Integritätsbereich und $I \neq 0$ ein Ideal von R. Das Ideal I ist genau dann ein projektiver Modul, wenn I invertierbar ist (d.h wenn es einen R-Untermodul I' von $K = \operatorname{Quot}(R)$ mit $II' = R$ gibt). Zusätzlich gilt: derartige Ideale sind endlich-erzeugt.*

Beweis: Sei $II' = R$ für einen R-Untermodul I' von K. Es gibt also $a_i \in I$, $b_i \in I'$ mit $\sum_{i=1}^n a_ib_i = 1$. Wegen $Ib_i \subseteq II' = R$ bildet die Rechtsmutiplikation $\cdot b_i$: ${}_RK \to {}_RK$ den R-Untermodul $I \subset K$ in $R \subset K$ ab, also erhalten wir einen Homomorphismus $\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$: $I \to R^n$ und die Komposition der beiden Abbildungen

$$I \xrightarrow{\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}} R^n \xrightarrow{[\,a_1 \,\dots\, a_n\,]} I$$

ist die Idenität. Also ist I isomorph zu einem direkten Summanden von R^n, also projektiv und endlich erzeugt.

Umgekehrt betrachten wir ein Ideal I, das projektiver Modul ist, es gibt also Homomorphismen f_i: $I \to R$ und g_i: $R \to I$ mit folgender Eigenschaft: Für jedes $x \in I$ sind fast alle $g_i(x) = 0$ und es ist $\sum_i g_if_i = 0$. Zu g_i gibt es a_i, $i \in I$ mit $g_i(r) = ra_i$ für alle $r \in R$.

Wir zeigen: Zu jedem f_i, $i \in T$ gibt es $b_i \in K$ mit $Ib_i \subseteq R$ und $f_i(y) = yb_i$ für alle $y \in I$, und es ist $f_i = 0$ für fast alle i. Zum Beweis wähle $0 \neq x \in I$. Ist $y \in I$, so ist

$$xf_i(y) = f_i(xy) = yf_i(x),$$

setzen wir also $b_i = \frac{f_i(x)}{x}$, so ist

$$f_i(y) = y \cdot \frac{f_i(x)}{x} = y \cdot b_i$$

für alle $y \in I$. Wegen $f_i(y) \in R$ für jedes $y \in I$ ist $Ib_i \subseteq R$. Da $f_i(x) = 0$ für fast alle i, ist $b_i = 0$ für fast alle i, also $f_i = 0$ für fast alle i. Ist also $\{1, 2, \ldots, n\}$ die Menge der $i \in I$ mit $f_i \neq 0$, so erhalten wir Abbildungen

$$I \xrightarrow{\left[\begin{smallmatrix} b_1 \\ \vdots \\ b_n \end{smallmatrix}\right]} R^n \xrightarrow{[\, a_1 \ \ldots \ a_n \,]} I$$

deren Komposition die Identität ist: also $\sum_{i=1}^n a_i b_i = 1$. Sei $I' = \langle b_1, \ldots, b_n \rangle$. Dann ist einerseits $1 \in II'$, also $R \subseteq II'$. Andererseits ist $II' = \sum_{i=1}^n Ib_i \subseteq R$. Beides zusammen zeigt $II' = R$.

Sei R ein Integritätsbereich. Man nennt einen Untermodul U von $\mathrm{Quot}(R)$ ein *gebrochenes Ideal*, wenn es von Null verschiedene Elemente a, b mit $\langle a \rangle \subseteq U \subseteq \langle b \rangle$ gibt.

Die Menge der gebrochenen Ideale von R bilden bezüglich der Multiplikation eine Halbgruppe mit Einselement R. Die von Null verschiedenen zyklischen gebrochenen Ideale (also Untermoduln von $\mathrm{Quot}(R)$ der Form $\langle a \rangle$ mit $0 \neq a \in K$) bilden eine Untergruppe (denn $\langle a \rangle \langle a^{-1} \rangle = R$).

Beachte: Sind U, U' Untermoduln von $K = \mathrm{Quot}(R)$ mit $UU' = R$, so sind dies gebrochene Ideale und es ist $U' = \{x \in K \mid Ux \subseteq R\}$. Beweis: Wir zeigen zuerst die zweite Behauptung. Sei also $V = \{x \in K \mid Ux \subseteq R\}$ natürlich gilt $U' \subseteq V$. Umgekehrt ist

$$V = RV = U'UV \subseteq U'R = U'.$$

Zur ersten Behauptung: Schreibe $1 = \sum_{i=1}^n a_i b_i$ mit $a_i \in U, b_i \in U'$. Sei $V = \langle b_1, \ldots, b_n \rangle \subseteq U'$, also $UV \subseteq UU' = R$. Wegen $1 \in UV$ ist auch $R \subseteq UV$, also $UV = R$ und demnach $V = U'$, also ist U' endlich erzeugt. Das Hauptnenner-Argument zeigt, daß U' in einem zyklischen Untermodul enthalten ist, natürlich ist $U' \neq 0$. Dies zeigt: U' is ist gebrochenes Ideal.

Teil III. Dedekind Ringe.

Satz. *Sei R ein Integritätsbereich. Die folgenden Eigenschaften sind äquivalent:*
(i) *Die Halbgruppe der gebrochenen Ideale ist eine Gruppe.*
(ii) *Jedes gebrochene Ideal ist invertierbar (d.h. es gibt einen Untermodul I' von* $\mathrm{Quot}(R)$ *mit $II' = R$).*
(iii) *Jedes von Null verschiedene Ideal von R ist invertierbar.*
(iii′) *Jedes Ideal von R ist projektiver Modul.*
(iv) *Jedes von Null verschiedene Ideal ist Produkt von maximalen Idealen.*
(v) *Jedes von Null verschiedene Ideal ist Produkt von Primidealen.*
(vi) *Jedes von Null verschiedene Primideal P ist invertierbar.*
(vii) *R ist noethersch, R_M ist Hauptidealring für jedes maximale Ideal M von R.*
(viii) *R ist noethersch, ganz abgeschlossen und hat Krull-Dimension höchstens 1.*

Zusatz: *Die Darstellung eines Ideals als Produkt von invertierbaren Primidealen ist bis auf die Reihenfolge eindeutig.*

Beweis: (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii): trivial. (ii) $\Longrightarrow$ (i): Wie wir gesehen haben, folgt aus $II' = R$, daß I' ebenfalls gebrochenes Ideal ist. (iii) $\Longrightarrow$ (ii). Sei I gebrochenes Ideal, etwa $\langle \frac{a}{\rangle} \subseteq I \subseteq \langle b\rangle$ mit $a, b \in K$. Sei $0 \neq r \in R$ mit $rb \in R$. Dann ist $Ir \subseteq \langle rb\rangle \subseteq R$ ein von Null verschiedenes Ideal von R. Es ist invertierbar, etwa $IrI' = R$. Also ist I invertierbar. Für (iii) $\Longleftrightarrow$ (iii') ist nur noch anzumerken, daß der Nullmodul natürlich projektiv ist.

(iv) $\Longrightarrow$ (iii). Sei M maximales Ideal, sei $0 \neq u \in M$. Schreibe $Ru = \prod_i M_i$ mit Prim-Idealen $M_1, \ldots, M_n$. Wegen $\prod M_i \subseteq M$ und M Primideal, folgt $M_i \subseteq M$ für ein i, also $M_i = M$. Wir können annehmen $i = 1$. Also $M \cdot \prod_{j\geq 2} M_j = Ru$, also $M \cdot (\prod_{j\geq 2} M_j)u^{-1} = R$. Dies zeigt, daß M invertierbar ist.

(iii) $\Longrightarrow$ (iv). Wir setzen also voraus, daß jedes von Null verschiedene Ideal I von R invertierbar ist. Insbesondere ist dann R noethersch. Angenommen, es gibt ein von Null verschiedenes Ideal, das sich nicht als Produkt von maximalen Idealen schreiben läßt; wähle I maximal mit dieser Eigenschaft. Das Ideal I ist ein echtes Ideal (denn nach Definition ist R Produkt von maximalen Idealen, mit 0 Faktoren), also in einem maximalen Ideal M enthalten, und zwar echt. Bilde $M^{-1}I$, dabei ist $M^{-1} = \{r \in K \mid rM \subseteq R\}$. Wegen $I \subseteq M$ ist $M^{-1}I \subseteq R$, also ein Ideal von R. Wegen $1 \in M^{-1}$ ist $I \subseteq M^{-1}I$. Wäre $I = M^{-1}I$, so wäre $MI = I$, dies ist aber unmöglich, wie wir gleich zeigen werden. Wegen $I \subset M^{-1}I$ läßt sich $M^{-1}I$ als Produkt maximaler Ideale schreiben, etwa $M^{-1}I = M_1 \cdots M_t$, also $I = M \cdot M_1 \cdots M_t$, ein Widerspruch zur Wahl von I.

Es bleibt zu zeigen: *Sei I endlich erzeugtes Ideal in einem Integritätsbereich R, sei M maximales Ideal von R mit $MI = I$. Dann ist $I = 0$.* Beweis: Sei $I = \sum_{i=1}^n Rx_i$. Sei $I_j = \sum_{i=j}^n Rx_i$, für $0 \leq j \leq n$, also $I_1 = I$, und $I_{n+1} = 0$. Wir konstruieren induktiv Elemente $z_j \in M$ mit $(1 - z_j)I \subseteq I_j$. Für $i = 1$ nimm $z_1 = 0$. Sei nun z_j konstruiert, also $(1-z_j)I \subseteq I_j$. Wegen $I \subseteq MI$ ist $(1-z_j)I \subseteq (1-z_j)MI \subseteq MI_j$, also $(1 - z_j)x_j = \sum_{i=j}^n r_{ij}x_i$ mit $r_{ij} \in M$. Also ist $(1 - z_j - r_{jj})x_j \in I_{j+1}$, also $(1 - z_j - r_{jj})I_j \in I_{j+1}$. Setze nun $(1 - z_{j+1}) = (1 - z_j - z_{jj})(1 - z_j)$. Es ist

$$(1 - z_{j+1})I = (1 - z_j - z_{jj})(1 - z_j)I \subseteq (1 - z_j - z_{jj})I_j \subseteq I_{j+1}.$$

Also erhalten wir mit $z = z_{n+1}$ ein Element in M mit $(1-z)I = 0$. Da R nullteilerfrei ist und $1 \neq z$, folgt $I = 0$.

(iv) $\Longrightarrow$ (v): trivial. Bevor wir nun (v) $\Longrightarrow$ (vi) zeigen, beweisen wir den Zusatz.

Beweis des Zusatzes: Sei $I = P_1 \cdots P_s = Q_1 \cdots Q_t$ mit invertierbaren Primidealen P_i, Q_j. Wähle P_i minimal unter den Idealen $P_1, \ldots P_s$. Wegen $Q_1 \cdots Q_t \subseteq P_1$ gibt es Q_j mit $Q_j \subseteq P_1$. Auch hier können wir annehmen $j = 1$. Wegen $P_1 \cdots P_s \subseteq Q_1$ gibt es P_i mit $P_i \subseteq Q_1$. Die Minimalität von P_1 und $P_i \subseteq Q_1 \subseteq P_1$ liefern $P_1 = Q_1$. Da wir voraussetzen, daß P_1 invertierbar ist, folgt nun $P_1 \cdots P_s = Q_2 \cdots Q_t$. Mit Induktion folgt die Behauptung.

Beweis der Implikation (v) $\Longrightarrow$ (vi). Wir zeigen als erstes: Aus (v) folgt: *jedes invertierbare Primideal ist maximal.* Sei also P invertierbares Primideal. Sei $a \in R \setminus P$. Wir zeigen $P + Ra = R$ (dies impliziert, daß P maximal ist).

Schreibe die Ideale $P+Ra = P_i \cdots P_r$ und $P+Ra^2 = Q_1 \cdots Q_s$ mit Primidealen P_i, Q_j. Wegen $P \subseteq P_1 \cdots P_r \subseteq \bigcap P_i$ gilt $P \subseteq P_i$ für jedes i; entsprechend $P \subseteq Q_j$ für jedes j. Im Faktorring $\overline{R} = R/P$ sind die Ideale P_i/P und Q_j/P Primideale und es gilt $\overline{R}\overline{a} = P_1/P \cdots P_r/P$ und $\overline{Ra^2} = Q_1/P \cdots Q_s/P = (P_1/P)^2 \cdots (P_r/P)^2$, also ist $s = 2r$ und wir können annehmen $Q_{2i-1}/P = Q_{2i}/P = P_i/P$, also auch $Q_{2i-1} = Q_{2i} = P_i$. Daraus folgt:

$$P + Ra^2 = Q_1 \cdots Q_s = (P_1 \cdots P_r)^2 = (P + Ra)^2.$$

Also gilt

$$P \subseteq P + Ra^2 = (P + Ra)^2 \subseteq P^2 + Ra.$$

Es gilt sogar $P \subseteq P^2 + Pa$, denn ist $p \in P$, so schreibe $p = y + za$ mit $y \in P^2, z \in R$, also $za \in P$. Wegen $a \notin P$ folgt $z \in P$. Die umgekehrte Inklusion ist trivial, also gilt

$$P = P^2 + Pa.$$

Nun ist P invertierbar, also ist $R = P + Ra$.

Nun also der eigentliche Beweis von (v) $\Longrightarrow$ (vi). Nimm ein Element $0 \neq p \in P$ und schreibe $Rp = \prod P_i$ mit Primidealen P_i. Alle diese Primideale P_i sind invertierbar (denn $Rp^{-1} \prod P_i = R$). Wegen $\prod P_i \subseteq P$ und P prim gibt es ein i mit $P_i \subseteq P$. Da P_i invertierbar ist, ist P_i maximal, also $P_i = P$ ist invertierbar.

Beweis (vi) $\Longrightarrow$ (iii). Sei $\mathcal{U}$ die Menge der von Null verschiedenen Ideale, die nicht invertierbar sind. Angenommen $\mathcal{U} \neq \emptyset$. Ist $(U_\lambda)_\lambda$ eine Kette (bezüglich Inklusion) in $\mathcal{U}$, so gehört auch $U = \bigcup U_\lambda$ zu $\mathcal{U}$ (denn wäre U invertierbar, so endlich erzeugt, also gleicbh einem U_λ, Widerspruch). Also wähle $U \in \mathcal{U}$ maximal (Zorn). Da U nicht invertierbar ist, ist U ein echtes Ideal von R. Da alle Primideale invertierbar sind, ist U kein Primideal. Also gibt es $a, b \in R \setminus U$ mit $ab \in U$. Setze $U' = \{x \in R \mid xa \in U\}$, dies ist ein Ideal von R mit $U \subseteq U'$. Wegen $b \in U' \setminus U$ gilt $U \subset U'$. Also ist U' invertierbar. Entsprechend ist $U \subset U + Ra$, also ist auch $U + Ra$ invertierbar. Mit U' ist auch $U'a$ als Produkt zweiter invertierbarer Ideale invertierbar. Andererseits ist $U'a = U \cap Ra$ (denn $U'a \subseteq U$ und $U'a \subseteq Ra$ folgen beide aus der Definition von U', Ist andererseits $u \in U \cap Ra$, etwa $u = ra$ mit $r \in R$, so ist $r \in U'$, also $u = ra \in U'a$.

Wir erhalten eine exakte Folge der Form

$$0 \to U \cap Ra \to U \oplus Ra \to U + Ra \to 0.$$

Da $U + Ra$ invertierbar, also projektiv ist, zerfällt die Folge und es gilt $U \oplus Ra \simeq (U \cap Ra) \oplus (U + Ra)$. Der rechte Modul ist projektiv, also ist auch U projektiv, Widerspruch.

Vorbemerkungen zum Beweis: (iii) $\implies$ (vii). Wir betrachten zuerst den Fall eines lokalen Rings.

Lemma. Sei R ein lokaler Integritätsbereich. Genau dann ist jedes von Null verschiedene Ideal invertierbar, wenn R ein Hauptidealring (also ein diskreter Bewertungsring oder ein Körper) ist.

Beweis: In Hauptidealbereichen ist jedes von Null verschiedene Ideal invertierbar. Umgekehrt sei jedes von Null verschiedene Ideal von R invertierbar. Dann ist jedes Ideal endlich erzeugt, also R ist noethersch. Es reicht zu zeigen: Sind x, y von Null verschiedene Elemente des Rings, so ist $x \in Ry$ oder $y \in Rx$. Sei $I = \langle x, y \rangle$ und $II' = R$, also $1 = xx' + yy'$ mit $x', y' \in I$. Wir sehen, daß gilt $Rxx' + Ryy' = R$, also, da R lokal ist, ist etwa $Ryy' = R$. Daraus folgt einerseits $Ryy'x = Rx$, andererseits ist $Rxy' \subseteq R$ und demnach $Rxy'y \subseteq Ry$. Insgesamt sehen wir also $Rx \subseteq Ry$.

Lemma. *Sei R Integritätsbereich mit* (iii). *Sei Σ multiplikative Menge von R. Dann gilt* (iii) *auch in $R\Sigma^{-1}$.*

Beweis: Sei I ein von Null verschiedenes Ideal von $S = R\Sigma^{-1}$. Dann ist $I = (I \cap R)\Sigma^{-1}$ (denn $\supseteq$ ist trivial, und ist $x = \frac{r}{s} \in I$ mit $r \in R, s \in \Sigma$, so ist $r = \frac{r}{s}s$ in $I \cap R$, also $\frac{r}{s} = rs^{-1} \in (I \cap R)\Sigma^{-1}$). Es ist $I \cap R$ ein von Null verschiedenes Ideal von R, also invertierbar: es gibt also einen R-Untermodul J mit $(I \cap R)J = R$. Also $R\Sigma^{-1} = (I \cap R)\Sigma^{-1}J\Sigma^{-1} = I \cdot J\Sigma^{-1}$ zeigt, daß I invertierbar ist.

Beweis von (iii) $\implies$ (vii): Ist jedes von Null verschiedene Ideal von R invertierbar, so R noethersch. Und für jedes maximale Ideal M von R gilt die Bedingung (iii) im Ring $R_M = R(R \setminus M)^{-1}$, also ist R_M ein Hauptidealring.

Vorbemerkungen zum Beweis (vii) $\implies$ (viii). Ganz allgemein gilt:

Lemma. *Sei R Integritätsbereich. Dann ist $R = \bigcup_M R_M$, wobei M alle maximalen Ideale durchläuft.*

Beweis: Eine Inklusion ist trivial. Sei also $x \in \bigcup R_M$. Sei $I = \{y \in R \mid yx \in R\}$, dies ist ein Ideal von R. Wäre dies ein echtes Ideal, so wäre es in einem maximalen Ideal enthälten, etwa in M. Da $x \in R_M$, schreiben wir $x = \frac{r}{s}$ mit $r \in R$ und $s \in R \setminus M$. Es ist $s \in I$, denn $sx = s\frac{r}{s} = r \in R\}$, also $s \in T \subseteq M$, Widerspruch. Demnach ist $I = R$, also $1 \in I$, also $x \in R$.

Lemma. *Ist R Integritätsbereich, und sind multiplikative Mengen Σ_i gegeben, mit $R = \bigcup R\Sigma_i^{-1}$, so gilt: Sind alle Ringe $R\Sigma_i^{-1}$ ganz abgeschlossen, so ist auch R ganz abegschlossen.*

Beweis: Sei $f(T) \in R[T]$ normiertes Polynom, sei $x \in K$ Nullstelle von $f(T)$. Dies ist ein normiertes Polynom in $R\Sigma_i^{-1}[T]$ und $x \in \mathrm{Quot}(R\Sigma_i{-}1)$. Da der Ring

$R\Sigma_i^{-1}$ ganz abgeschlossen ist, ist $x \in R\Sigma_i^{-1}$, also im Durchschnitt dieser Unterringe, also in R.

Nun der Beweis (vii) $\implies$ (viii): Die beiden Lemmata zeigen, daß aus R_M ganz abgeschlossen für alle M folgt, daß auch R ganz abgeschlossen ist. Jede Primidealkette liefert eine entsprechend lange Primidealkette in einem Ring R_M. Da alle Ringe R_M Krull-Dimension höchstens 1 haben, hat auch R Krull-Dimension höchstens 1.

Beweis von (viii) $\implies$ (vi). Sei $P \neq 0$ Primideal von R, sei $0 \neq a \in P$. In einem noetherschen Ring enthält jedes Ideal ein Produkt von Primidealen, die von Null verschieden sind. Also gibt es Primideale $P_1, \dots, P_t$ mit $P_1 \cdots P_t \subseteq Ra$. Wähle eine solche Darstellung mit t minimal. Wegen $P_1 \cdots P_t \subseteq Ra \subseteq P$ und P prim gibt können wir annehmen $P_1 \subseteq P$. Wegen Krull-Dimension höchstens 1 ist P_1 maximales Ideal, also $P_1 = P$. Die Minimalität von t besagt $P_2 \dots P_t \not\subseteq Ra$, also gibt es $b \in P_1 \cdots P_t$ mit $b \notin Ra$.

Wegen $bP \subseteq Ra$ ist $a^{-1}bP \subseteq R$. Sei $I = \{x \in K \mid xP \subseteq R\}$. Es ist $P \subseteq IP$ (wegen $1 \in I$) und $IP \subseteq R$ (nach Definition von I). Da P maximal ist, gibt es nur die Möglichkeiten $P = IP$ und $IP = R$. Letzteres hätten wir gern, denn dies zeigt ja, daß P invertierbar ist. Angenommen, $P = IP$. Da $a^{-1}b \in I$, gilt $a^{-1}bP \subseteq P$, aber dann ist $a^{-1}b$ ganz über R (daran sei gleich noch erinnert), gehört also zu R und demnach ist $b = (a^{-1}b)a \in Ra$, ein Widerspruch.

Erinnerung. *Sei $R \subseteq S$ eine Inklusion von Integritätsbereichen und sei $U \neq 0$ ein endlich erzeugter R-Untermodul von S. Ist $s \in S$ mit $sU \subseteq U$, so ist s ganz über R.*

Beweis: Sei $u_1, \dots, u_n$ ein R-Erzeugendensystem von U, schreibe $cu_i = \sum r_{ij}u_j$ mit $r_{ij} \in R$, also $\sum (c\delta_{ij} - r_{ij})u_j =$. Betrachte die Matrix $A = (r_{ij})$ und auch $(cI - A)$ Multiplizieren wir mit der klassischen Adjunkten $\operatorname{adj}(cI - A)$, so erhalten wir $\chi_A(c)u_j = 0$, für alle j. Da $U \neq 0$, gilt $u_j \neq 0$ für mindestens ein j und demnach $\chi_A(c) = 0$, also ist c Nullstelle des charakteristischen Polynoms der Matrix A.

Bemerkung (ohne Beweis): "Jedes Ideal ist projektiv" bedeutet: Jeder Untermodul von ${}_RR$ ist projektiv. Daraus folgt ganz allgemein: Jeder Untermodul eines projektiven Moduls ist projektiv; man nennt derartige Ringe *erblich.*

Ist R Dedekind-Ring, so ist die Gruppe der gebrochenen Ideale freie abelsche Gruppe mit Basis die Menge der maximalen Ideale. (Freie abelsche Gruppe = freier $\mathbb{Z}$-Modul).

Dies folgt aus der Eindeutigkeit der Darstellung als Produkt invertierbarer Primideale.

Zerlegungssatz: Weitreichende Verallgemeinerung des Fundamentalsatzes der Algebra und des Fundamentalsatzes der elementaren Zahlentheorie.

In einem Dedekind-Ring bezeichnet man die Faktorgruppe der Gruppe der gebrochenen Ideale modulo der Untergruppe der zyklischen gebrochenen Ideale als

Idealklassengruppe, ihre Ordnung die *Klassenzahl.* Wichtig in der Zahlentheorie: *Die Idealklassengruppe ist eine endliche Gruppe.* Natürlich gilt: Genau dann ist die Idealklassengruppe trivial, wenn R ein Hauptidealring ist. Die Idealklassengruppe mißt die Abweichung, ein Hauptidealring zu sein.

Sei $h(m)$ die Klassenzahl des imaginär-quadratischen Zahlkörpers $K = \mathbb{Q}[\sqrt{m}]$. Genau dann ist $h(m) = 1$, wenn gilt

$$|m| = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

(die List der zugehörenden "Diskriminanten" ist $|d| = 3, 4, 7, 8, 11, 19, 43, 76, 163$). (Ferner gibt es genau 18 Fälle mit Klassenzahl 2.) Es gibt viele, möglicherweise unendlich viele reell-quadratische Zahlkörper mit Klassenzahl 1.

Lemma. (Fast wie oben) *Ist $I \subseteq K$ ein Untermodul, so ist jeder R-Homomorphismus $f\colon I \to K$ von der Form $f(x) = x \cdot b$ mit $b \in K$.*

Beweis: Ist $I = 0$, so nimm $b = 0$. Sei also $I \neq 0$. Dann ist auch $I \cap R \neq 0$ and wir wählen ein Element $0 \neq u \in I \cap R$. Ist $y \in I$, etwa $y = \frac{r}{s}$ mit $r, s \in R$, so ist

$$suf(\frac{r}{s}) = f(su\frac{r}{s}) = f(ur) = rf(u),$$

also gilt für $b = \frac{f(u)}{u}$

$$f(y) = f(\frac{r}{s}) = \frac{r}{s} \cdot \frac{f(u)}{u} = y \cdot b.$$

Die invertierbaren gebrochenen Ideale sind gerade die "projektiven Moduln vom Rang 1", wir sehen also: Zwei projektive Moduln vom Rang 1 sind genau dann isomorph, wenn sie zur gleichen Restklasse modulo der Untergruppe der zyklischen gebrochenen Ideale gehören (und die Multiplikation entspricht gerade dem Tensor-Produkt). Man bezeichnet mit $\mathrm{Pic}(R)$ die Gruppe der Isomorphieklassen projektiver Moduln vom Rang 1 bezüglich des Tensorprodukts. Wir sehen also: *Für einen Integritätsbereich R gilt:* $\mathrm{Pic}(R)$ *ist gleich der Restklassengruppe der invertierbaren gebrochenen Ideale modulo der Untergruppe der zyklischen gebrochenen Ideale.*