5. Die Idealtheorie in Dedekind-Ringen.

Das Multiplizieren von Idealen: Seien I, J Ideale. Setze $IJ = \sum x_i y_i$ mit $x_i \in I, y_i \in J$. Dies ist wieder ein Ideal. Ist R Bereich und sind I, J von Null verschiedene Ideale, so ist auch IJ wieder von Null verschieden. Sind I, J endlich erzeugt, so ist auch IJ endlich erzeugt. Sei $\mathcal{I}$ die Menge der von Null verschiedenen endlich erezugten Ideale. Offensichtlich gilt: *Die Menge $\mathcal{I}$ ist mit der Idealmultiplikation eine kommutative Halbgruppe mit R als neutralem Element.*

Entsprechend können wir für einen Bereich R mit Quotientenkörper K die Menge $\mathcal{J}$ der von Null verschiedenen endlich erzeugten R-Untermoduln von K betrachten, man nennt derartige Untermoduln *gebrochene Ideale.* Die Multiplikation $\cdot$ für gebrochene Ideale wird in gleicher Weise definiert und man sieht: *Die Menge $\mathcal{J}$ ist mit $\cdot$ eine kommutative Halbgruppe mit neutralem Element R.*

Bezeichnen wir mit $\mathcal{P}$ die Menge der zyklischen von Null verschiedenen R-Untermoduln von K, so ist $\mathcal{P}$ eine Unterhalbgruppe von $\mathcal{J}$, und selbst eine Gruppe; sie ist isomorph zu $K^*/U(R)$; dabei steht K^* für die multiplikative Gruppe des Körpers K und $U(R)$ für die Einheitengruppe des Rings R (den Isomorphismus erhält man durch die kanonische Abbildung $x \mapsto Rx$ für $x \in K^*$).

Erinnerung: Ein Element h einer multiplikativen Halbgruppe H heißt *invertierbar*, wenn es ein $h' \in H$ gibt mit $hh' = 1$; man schreibt dann $h' = h^{-1}$. Wir interessieren uns für die Frage, welche gebrochenen Ideale I invertierbar sind (das heißt: invertierbar in $\mathcal{J}$); vor allem haben wir dabei Ideale ($\neq 0$) im Auge. Warnung: wenn von der Invertierbarkeit eines Ideals I die Rede ist, so meint man die Invertierbarkeit in $\mathcal{J}$, und nicht etwa in $\mathcal{I}$).

Ist $I \in \mathcal{J}$, so setze $I^{(-1)} = \{x \in K \mid Ix \subseteq R\}$. Dies ist immer ein R-Untermodul von K und immer von Null verschieden (denn ist $I = \sum_{i=1}^n Rx_i$ mit $x_i \in K$, etwa $x_i = \frac{r_i}{s}$ mit $r_1, \ldots, r_n, s \in R$ und $s \neq 0$, so ist $s \in I^{(-1)}$. Im allgemeinen ist aber nicht klar, ob $I^{(-1)}$ endlich erzeugt ist. Wie wir gleich sehen werden, ist dies zumindest dann der Fall, wenn $II^{(-1)} = R$ gilt. Imm gilt $II^{(-1)} \subseteq R$, es ist also $II^{(-1)}$ ein Ideal von R. (In vielen Büchern wird statt $I^{(-1)}$ einfach I^{-1} geschrieben, auch wenn I nicht invertierbar ist, das kann aber irreführend sein.)

5.1. *Sei I gebrochenes Ideal.*

(a) *Ist I invertierbar, so ist $I^{-1} = I^{(-1)}$.*

(b) *Gilt $II^{(-1)} = R$, so ist $I^{(-1)}$ endlich erzeugt,* also in $\mathcal{J}$ und damit ist I invertierbar.

Beweis. (a) Sei $I^{-1} \in \mathcal{J}$ das inverse Element zu I. Wegen $II^{-1} = R$ gilt $Ix \subseteq R$ für jedes $x \in I^{-1}$, also ist $I^{-1} \subseteq I^{(-1)}$. Wegen $1 \in II^{-1}$ gibt es $a_i \in I, y_i \in I^{-1}$ mit $\sum_i a_i b_i = 1$. Ist nun $x \in I^{(-1)}$, so ist $x = x \sum_i a_i b_i = \sum_i (a_i x) b_i \in \sum_i Rb_i \subseteq I^{-1}$. Also gilt auch $I^{(-1)} \subseteq I^{-1}$.

(b) Wegen $I^{(-1)} I = R$ lässt sich das Einselement in folgender Form darstellen: $1 = \sum_{i=1}^n x_i y_i$ mit $x_i \in I^{-1}$ und $y_i \in I$. Wegen $y_i \in I$ ist $\sum Ry_i \subseteq I$. Ist $z \in I$, so ist $z = z \cdot 1 = \sum z x_i y_i \in \sum Ry_i$, denn $x_i \in I^{-1}, z \in I$ liefert $zx_i \in R$.

Hier ein Beispiel eines nicht-invertierbaren Ideals: Sei $R = k[X^2, X^3]$ und $I = RX^2 + RX^3$. Natürlich gilt $K = \mathrm{Quot}(R) = k(X)$. Man sieht unmittelbar: Es ist $k[X] \subseteq I^{(-1)}$. Wegen $RX^2 \subseteq I$ gilt $I^{(-1)} \subseteq (RX^2)^{(-1)} = RX^{-2}$, also

$$k[X] \subseteq I^{(-1)} \subseteq RX^{-2}.$$

Da die Folge $1, X^2, X^3, X^4, \ldots$ eine Basis von R ist, ist $X^{-2}, 1, X, X^2, \ldots$ eine Basis von RX^{-2}. Nun ist aber X^{-2} nicht in $I^{(-1)}$, denn $X = X^3X^{-2}$ liegt nicht in R. Daraus folgt $k[X] = I^{(-1)}$ und demnach ist $II^{(-1)} = Ik[X] = I$ eine echte Teilmenge von R.

5.2. *Sei P ein maximales Ideal in einem noetherschen Bereich der Dimension 1. Dann ist $R \subset P^{-1}$ eine echte Inklusion.*

Beweis: Wegen $1 \in P^{-1}$ ist $R \subseteq P^{-1}$. Sei $0 \neq a \in P$. Nach 3.1 gibt es maximale Ideale $P_1, \ldots, P_t$ mit $P_1 \cdots P_t \subseteq Ra$. Wähle solche maximale Ideale mit t minimal. Aus $P_1 \cdots P_t \subseteq P$ folgt, $P_i = P$ für mindestens einen Faktor P_i, etwa $P_1 = P$. Wegen der Minimalität von t ist $P_2 \cdots P_t \not\subseteq Ra$. Also gibt es ein $b \in P_2 \cdots P_t$ mit $b \notin Ra$. Es ist $Pb = P_1 b \subseteq Ra$, also $Pba^{-1} \subseteq P$ und demnach ist $ba^{-1} \in P^{-1}$. Wegen $b \notin Ra$ ist aber $ba^{-1} \notin R$. Also haben wir ein Element gefunden, das zu P^{-1}, aber nicht zu R gehört.

5.3. Sei nun R ein Dedekind-Ring. *Ist $I \neq 0$ Ideal, und $P \neq 0$ Primideal, so ist $I \subset IP^{-1}$ eine echte Inklusion.*

Beweis. Wegen $1 \in P^{-1}$ ist $I \subseteq IP^{-1}$. Angenommen, $I = IP^{-1}$. Ist $\alpha \in P^{-1}$, so haben wir $I\alpha \subseteq I$, also ist α ganz über R und demnach wegen der Normalität in R. Es ist also $P^{-1} \subseteq R$, im Gegensatz zu (c).

5.4. In einem Dedekind-Ring gilt: *Jedes maximale Ideal M ist invertierbar.*

Beweis: Es ist $M \subset MM^{-1} \subseteq R$. Die Maximalität impliziert $MM^{-1} = R$.

5.5. Satz. *Sei R ein Dedekind-Ring. Dann gilt: Jedes von Null verschiedene Ideal ist Produkt von maximalen Idealen und ist invertierbar.*

Beweis: Nur die erste Aussage ist noch zu beweisen, da wir schon wissen, dass maximale Ideale (und damit auch Produkte maximaler Ideale) invertierbar sind. Angenommen, es gibt ein Ideal $I \neq 0$, das sich nicht als Produkt von maximalen Idealen schreiben lässt. Da R noethersch ist, können wir I maximal wählen. Die übliche Konvention von leeren Produkten besagt: $I \neq R$, also ist $I \subseteq M$ für ein maximales Ideal M. Bilde $I' = IM^{-1}$. Es ist $I' = IM^{-1} \subseteq MM^{-1} \subseteq R$, also ein Ideal von R. Wegen (d) ist $I \subset I'$. Die Maximalität von I besagt, dass wir I' als Produkt von maximalen Idealen schreiben können, etwa $I' = M_1 \cdots M_t$. Also $I = IR = IM^{-1}M = I'M = M_1 \cdots M_t M$. Widerspruch.

Daraus folgt aber auch, dass jedes von Null verschiedene Ideal I invertierbar ist: Schreibe $I = M_1 \cdots M_t$ mit maximalen Idealen M_i. Dann ist $IM_1^{-1} \cdots M_t^{-1} = M_1 \cdots M_t M_1^{-1} \cdots M_t^{-1} = R$.

5.6. Eindeutigkeit. *Sei R ein Bereich, seien $M_1, \dots, M_m$ invertierbare maximale Ideale, seien $N_1, \dots, N_n$ maximale Ideale. Gilt $M_1 \cdots M_m = N_1 \cdots N_n$, so ist $m = n$ und es gibt eine Permuation σ von m mit $M_i = N_{\sigma(i)}$ für alle i.*

Beweis mit Induktion nach m. Ist $m = 0$, so ist die Faktorisierung $R = N_1 \cdots N_n$ mit maximalen Idealen N_i gegeben. Wäre $n \geq 1$, so ware $R \subseteq N_1$, dies ist unmöglich. Also ist auch $n = 0$. Sei nun $m \geq 1$. Da das Produkt $N_1 \cdots N_n$ im Primideal M_1 enthalten ist, gibt es ein i mit $N_i \subseteq M_1$, und wir können annehmen $i = 1$. Da N_1 maximales Ideal ist, folgt $N_1 = M_1$. Da M_1 invertierbar ist, multiplizieren wir beide Seiten von $M_1 \cdots M_m = N_1 \cdots N_n$ mit M_1 und erhalten $M_2 \cdots M_m = N_2 \cdots N_n$. Nach Induktion ist nun $m - 1 = n - 1$ und es gibt die gewünschte Permutation.

Ist A eine Menge, so sei $\mathbb{Z}^{(A)}$ die Menge der Abbildungen $A \to \mathbb{Z}$ mit endlichem Träger. Dies ist bezüglich punktweiser Addition eine kommutative Gruppe, die *freie Gruppe* mit Basis A.

Folgerung. *Sei $\mathcal{M}$ die Menge der maximalen Ideale von R. Ordnen wir $e\colon \mathcal{M} \to \mathbb{Z}$ in $\mathbb{Z}^{(A)}$ das gebrochene Ideal $\prod_{M \in \mathcal{M}} M^{e(M)}$ zu, so erhalten wir einen Gruppen-Isomorphismus*

$$\eta\colon \mathbb{Z}^{(A)} \longrightarrow \mathcal{J}.$$

Die Gruppe $\mathcal{J}$ ist also freie Gruppe mit Basis $\mathcal{M}$. *Unter η wird die Unterhalbgruppe $\mathbb{N}_0^{(A)}$ der Abbildungen $A \to \mathbb{N}_0$ mit endlichem Träger auf die Unterhalbgruppe $\mathcal{I}$ von $\mathcal{J}$ abgebildet.*

Beweis: Ist $J \in \mathcal{J}$, etwa $J = \sum_{i=1}^t Rx_i$ mit $0 \neq x_i \in K$, so schreibe $x_i = \frac{r_i}{s}$ mit $r_1, \dots, r_t, s \in R$. Das Ideal $I = \sum_{i=1}^t Rr_i$ gehört zu $\mathcal{I}$, ist also Produkt maximaler Ideale, entsprechend ist $Rs \in \mathcal{I}$, also auch Produkt maximaler Ideale. Sei etwa $I = P_1 \cdots P_m$, $Rs == Q_1 \cdots Q_{m'}$ mit maximalen Idealen P_i, Q_j. Dann ist

$$J = I \cdot (Rs)^{-1} = P_1 \cdots P_m Q_1^{-1} \cdots Q_{m'}^{-1}.$$

Dies zeigt, dass sich jedes $J \in \mathcal{J}$ als Produkt von maximalen Idealen und deren Inversen schreiben lässt. Damit ist gezeigt, dass η surjektiv ist. Um die Injektivität zu zeigen, brauchen wir nur zu verifizieren, dass der Kern von η nur aus der Null-Abbildung besteht. Dies ist aber gerade die Behauptung 5.6.

Die Umkehrabbildung von η wird häufig gebraucht: Ist J ein gebrochenes Ideal und zwar $J = \prod_{P \in \mathcal{M}} P^{e(M)}$, so schreibt man $\operatorname{ord}_P(J) = e(P)$, und nennt dies die *$P$-Ordnung* von J. Für jedes $j \in \mathcal{J}$ gilt also

$$J = \prod\nolimits_{P \in \mathcal{M}} P^{\operatorname{ord}_P(J)}.$$

Beachte, dass für ein gebrochenes Ideal J gilt: *Genau dann ist $J \in \mathcal{I}$, wenn* $\operatorname{ord}_P(J) \geq 0$ *für alle $P \in \mathcal{M}$ gilt.* (Ist $\operatorname{ord}_P(J) \geq 0,$, so ist J ein Produkt von Primidealen, also insbesondere ein Ideal. Sei umgekehrt $J \neq 0$ ein Ideal, schreibe $J = P_1 \cdots P_t$

mit maximalen Idealen P_i. Dann ist $\mathrm{ord}_P(J)$ die Anzahl der Indizes $1 \le i \le t$ mit $P = P_i$, also $\mathrm{ord}_P(J) \ge 0$.)

Die Gruppe $\mathbb{Z}^{(A)}$ besitzt eine Halbordnungsstruktur: Sind $e, e' \colon A \to \mathbb{Z}$ Abbildungen mit endlichem Träger, so setze man $e \le e'$ falls $e(a) \le e'(a)$ für alle $a \in A$ gilt. Auch $\mathcal{J}$ besitzt eine Halbordnungstruktur, nämlich die mengentheoretische Inklusion. Diese beiden Halbordnungsstrukturen sind zueinander invers, denn es gilt: *Genau dann ist $J \subseteq J'$, wenn für alle $P \in \mathcal{M}$ gilt* $\mathrm{ord}_P(J) \ge \mathrm{ord}_P(J')$.

Insbesondere sehen wir

$$\mathrm{ord}_P(J + J') = \min\{\mathrm{ord}_P(J), \mathrm{ord}_P(J')\},$$
$$\mathrm{ord}_P(J \cap J') = \max\{\mathrm{ord}_P(J), \mathrm{ord}_P(J')\}.$$

Ein Beispiel: Die Faktorisierungen von 21 in $\mathbb{Z}[\sqrt{-5}]$. Wir betrachten also $K = \mathbb{Q}[\sqrt{-5}]$, es ist $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ (denn $-5 \equiv 3 \mod 4$).

Wir analysieren die Faktorisierungen

$$3 \cdot 7 = 21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Die Norm-Abbildung ist $N(a+b\sqrt{-5}) = a^2+5b^2$. Offensichtlich gilt: *Invertierbare Elemente in $\mathcal{O}_K$ sind nur $1, -1$.*

Offensichtlich gilt: $3, 7$ *sind keine Normen.* Man kann natürlich gleich alle möglichen Normen notieren (aber wir brauchen das gar nicht):

	5	20	45	$\cdots$
1	6	21	46	
4	9	24		
9	14	29		
16	21	36		
25	30			
$\vdots$				

Nun ist:

$$N(3) = 9, \quad N(7) = 49, \quad N(1 + 2\sqrt{-5}) = \quad N(1 + 2\sqrt{-5}) = 21,$$

also sehen wir: *Die Elemente* $3, 7, 1 + 2\sqrt{-5}, 1 - 2\sqrt{-5}$ *sind irreduzibel* (denn für eine Faktorisierung von $3 = \alpha\beta$ mit α, β nicht invertierbar, gilt: $N(\alpha)N(\beta)$ ist nichttriviale Faktorisierung von $N(3)$, usw.

Da die einzigen invertierbaren Elemente $1, -1$ sind, gilt: *die Elemente* $3, 7, 1 + 2\sqrt{-5}, 1 - 2\sqrt{-5}$ *sind paarweise nicht assoziiert.*

Bilde die Ideale

$$P_1 = \langle 3, 1+2\sqrt{-5}\rangle, \quad P_2 = \langle 3, 1-2\sqrt{-5}\rangle, \quad P_3 = \langle 7, 1+2\sqrt{-5}\rangle, \quad P_4 = \langle 7, 1-2\sqrt{-5}\rangle.$$

Behauptung: *Dies sind maximale Ideale.* Wir zeigen: die Abbildungen

$$\begin{aligned}
\eta_1 &: \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}/3 \quad \text{mit} \quad a + b\sqrt{-5} \mapsto \overline{a+b},\\
\eta_2 &: \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}/3 \quad \text{mit} \quad a + b\sqrt{-5} \mapsto \overline{a-b},\\
\eta_3 &: \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}/7 \quad \text{mit} \quad a + b\sqrt{-5} \mapsto \overline{a+3b},\\
\eta_4 &: \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}/7 \quad \text{mit} \quad a + b\sqrt{-5} \mapsto \overline{a-3b},
\end{aligned}$$

sind Ring-Homomorphismen: Klar ist die Aditivität, und dass $\eta_i(1) = 1$ gilt. Zu zeigen ist die Multiplikativität. Es ist

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5},$$

unter η_1 erhalten wir

$$ac - 5bd + ad + bc \equiv ac + bd + ad + bc = (a + b)(c + d) \mod 3.$$

Unter η_2 erhalten wir entsprechend

$$ac - 5bd - ad - bc \equiv ac + bd - ad - bc = (a - b)(c - d) \mod 3.$$

Unter η_3 erhalten wir

$$ac - 5bd + 3ad + 3bc \equiv ac + 9bd + 3ad + 3bc = (a + 3b)(c + 3d) \mod 7,$$

analog für η_4.

Offensichtlich gilt $P_i \subseteq \mathrm{Ker}(\eta_i)$, also sind die P_i echte Ideale. Wir haben die Inklusionskette

$$\langle 3\rangle \subset P_1 \subseteq \mathrm{Ker}(\eta_1) \subset \mathcal{O}_K,$$

mit zwei echten Inklusionen. Da $|\mathcal{O}_K/\langle 3\rangle| = 9$, folgt die Gleichheit $P_1 \subseteq \mathrm{Ker}(\eta_1)$.

Wichtig ist: *Es gilt*

$$\langle 3\rangle = P_1P_2, \quad \langle 7\rangle = P_3P_4, \quad \langle 1 + 2\sqrt{-5}\rangle = P_1P_3, \quad \langle 1 - 2\sqrt{-5}\rangle = P_2P_4.$$

Klar ist jeweils die Inklusion $\supseteq$. Die umgekehrte Inklusion folgt jeweils aus der Gleichheit:

$$(1 + 2\sqrt{-5})(1 + 2\sqrt{-5}) = 21 = 3 \cdot 7.$$

Wir verstehen nun die Zerlegung von 21:

$$\begin{array}{cccc}
(P_1P_2)(P_3P_4) = \langle 21\rangle = & (P_1P_3) & & (P_2P_4)\\
\langle 3\rangle \quad \langle 7\rangle & = \langle 21\rangle = \langle 1 + 2\sqrt{-5}\rangle & \langle 1 - 2\sqrt{-5}\rangle. &
\end{array}$$