Definition der Diskriminante

Sei K ein Zahlkörper, also eine endliche Körpererweiterung von $\mathbb{Q}$. Sei $b_1, \ldots, b_n$ eine Basis von K als $\mathbb{Q}$-Vektorraum.

Dann heißt die rationale Zahl

$$D(b_1, \ldots, b_n) := \det \begin{pmatrix} \mathrm{tr}_{K/\mathbb{Q}}(b_1 b_1) & \cdots & \mathrm{tr}_{K/\mathbb{Q}}(b_1 b_n) \\ \vdots & & \vdots \\ \mathrm{tr}_{K/\mathbb{Q}}(b_n b_1) & \cdots & \mathrm{tr}_{K/\mathbb{Q}}(b_n b_n) \end{pmatrix}$$

die *Diskriminante von K über $\mathbb{Q}$ zur Basis $b_1, \ldots, b_n$*.

Eigenschaften der Diskriminante

Verhalten der Diskriminante unter Basistransformation

Seien $b_1, \ldots, b_n$ und $b'_1, \ldots, b'_n$ zwei Basen von K als $\mathbb{Q}$-Vektorraum. Dann gilt für die zugehörigen Diskriminanten

$$D(b'_1, \ldots, b'_n) = (\det A)^2 D(b_1, \ldots, b_n),$$

wobei $A = (a_{ij})_{ij} \in \mathbb{Q}^{n \times n}$ die zu den beiden Basen gehörige Basiswechselmatrix (definiert durch die Forderungen $b'_i = \sum_j a_{ij} b_j$ für alle $i = 1, \ldots, n$) ist.

Dadurch motiviert definiert man noch folgenden Begriff: Die *Diskriminante von K über $\mathbb{Q}$* (ohne eine spezielle Basis zu nennen) ist die rationale Zahl

$$\mathrm{disc}_{K/Q} := D(b_1, \ldots, b_n),$$

wobei $b_1, \ldots, b_n$ eine beliebige Basis von K über $\mathbb{Q}$ ist. Das Ergebnis ist nicht wohldefiniert (hängt nämlich von der speziellen Wahl der Basis ab); man ergänzt die Definition daher noch um den Zusatz, dass man zwei Diskriminanten genau dann als gleich ansieht, wenn sie sich nur durch einen quadratischen Faktor unterscheiden. Die Rechenregel für die Basistransformation zeigt dann, dass diese Definition sinnvoll ist.

Diskriminante bei ganz-algebraischen Basisvektoren

Die Diskriminante ist stets eine rationale Zahl. Sind die b_i sogar ganz-algebraische Zahlen (das bedeutet, dass die b_i sogar eine normierte Polynomgleichung mit ganzzahligen Koeffizienten erfüllen), dann ist die Diskriminante sogar eine ganze Zahl. (Die Umkehrung gilt nicht.)

Das liegt daran, weil dann schon die Spuren $\mathrm{tr}_{K/\mathbb{Q}}(b_i b_j)$ jeweils ganze Zahlen sind.

Berechnung der Diskriminante

Kennt man ein primitives Element z von K, d. h. ein Element $z \in K$ mit $K = \mathbb{Q}(z)$, so kann man die Diskriminante $D(b_1, \ldots, b_n)$ einer Basis $b_1, \ldots, b_n$ wie folgt berechnen:

Zunächst sucht man sich Polynome $B_i \in \mathbb{Q}[X]$ mit $b_i = B_i(z)$. Solche muss es nach Voraussetzung immer geben. Dann gilt für die Diskriminante

$$D(b_1, \ldots, b_n) = \left(\det \begin{pmatrix} B_1(z_1) & \cdots & B_1(z_n) \\ \vdots & & \vdots \\ B_n(z_1) & \cdots & B_n(z_n) \end{pmatrix} \right)^2,$$

wobei $z_1, \ldots, z_n$ die galoissch Konjugierten von z in $\overline{\mathbb{Q}}$ sind.

Beispiel

Sei $K = \mathbb{Q}(z)$ mit $z = \sqrt[3]{2}$. Wir wollen die Diskriminante der Basis $(b_1, b_2, b_3) = (1, z, z^2)$ bestimmen.

Dazu setzen wir $B_1 := 1$, $B_2 := X$ und $B_3 := X^2$, denn dann gilt $B_1(z) = b_1$, $B_2(z) = b_2$ und $B_3(z) = b_3$.

Das Minimalpolynom von z ist $X^3 - 2$, also sind die galoissch Konjugierten von z die Zahlen z, ωz und $\omega^2 z$, wobei $\omega = e^{2\pi i/3}$.

Folglich ergibt sich die Determinante als

$$D(b_1, b_2, b_3) = \left(\det \begin{pmatrix} 1 & 1 & 1 \\ z & \omega z & \omega^2 z \\ z^2 & \omega^2 z^2 & \omega^4 z^2 \end{pmatrix} \right)^2 = -108.$$

Nutzen der Diskriminante

Die Diskriminante kann man nutzen, um zu beweisen, dass eine Vermutung für eine Ganzheitsbasis in der Tat korrekt ist. Denn Hilfssatz 7.128 (auf Seite 336) garantiert folgendes:

> Sei $K \supseteq \mathbb{Q}$ ein Zahlkörper. Sei $b_1, \ldots, b_n$ eine Basis von K als $\mathbb{Q}$-Vektorraum aus ganz-algebraischen Zahlen, also aus Elementen aus $\mathcal{O}_K$. Dann gilt:
>
> $$\mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n \subseteq \mathcal{O}_K \subseteq \mathbb{Z}\frac{1}{d}b_1 + \cdots + \mathbb{Z}\frac{1}{d}b_n,$$
>
> wobei $d = D(b_1, \ldots, b_n)$.

Möchte man also zeigen, dass $b_1, \ldots, b_n$ sogar eine Ganzheitsbasis ist (und nicht nur eine Basis über $\mathbb{Q}$, die zufälligerweise aus ganz-algebraischen Zahlen besteht), muss man also nur noch zeigen, dass alle Zahlen $x \in \mathcal{O}_K$ mit $x \in \mathbb{Z}\frac{1}{d}b_1 + \cdots + \mathbb{Z}\frac{1}{d}b_n$ schon in $\mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n$ liegen.

Beispiel

Wir wollen eine Ganzheitsbasis von $K = \mathbb{Q}(z)$ mit $z = \sqrt{-3}$ bestimmen. Eine Basis von K über $\mathbb{Q}$ ist durch $1, z$ gegeben; da z als Nullstelle des ganzzahligen Polynoms $X^2 + 3$ ganz-algebraisch ist, ist also folgendes unsere erste Vermutung:

1. Vermutung: Eine Ganzheitsbasis von $\mathcal{O}_K$ ist $1, z$.

Nun gibt es zwei Möglichkeiten zu sehen, dass diese Vermutung falsch sein muss. Die eine besteht darin, zu beobachten, dass die Zahl $(1 + z)/2$ trotz des gegenteiligen Anscheins auch ganz-algebraisch ist (nämlich als Nullstelle des Polynoms X^2-X+1), andererseits aber sicher keine ganzzahlige Linearkombination von 1 und z ist.

Eine andere besteht darin, zunächst mit dem nächsten Schritt weiterzumachen und dann zu erkennen, dass dieser fehlschlägt. In jedem Fall werden wir zu einer neuen Vermutung gelenkt:

2. Vermutung: Eine Ganzheitsbasis von $\mathcal{O}_K$ ist $(b_1, b_2) = (1, (1 + z)/2)$.

Um diese Vermutung zu überprüfen, berechnen wir zunächst die Diskriminante dieser Basis (Basis über $\mathbb{Q}$ ist sie definitiv). Dazu wählen wir (mit der Notation von oben) $B_1 := 1$, $B_2 := (1 + X)/2$, die galoissch Konjugierten von z sind z und $-z$. Somit gilt:

$$D(b_1, b_2) = \left(\det \begin{pmatrix} 1 & 1 \\ (1+z)/2 & (1-z)/2 \end{pmatrix}\right)^2 = -3.$$

Sei dann ein beliebiges Element $x \in \mathcal{O}_K$ gegeben. Wir wollen zeigen, dass $x \in \mathbb{Z}b_1 + \mathbb{Z}b_2$; und nach dem zitierten Hilfssatz wissen wir schon, dass $x \in \mathbb{Z}\frac{1}{3}b_1 + \mathbb{Z}\frac{1}{3}b_2$, dass es also ganze Zahlen $a, b \in \mathbb{Z}$ mit

$$x = \frac{1}{3}a + \frac{1}{3}b \cdot \frac{1 + \sqrt{-3}}{2}$$

gibt. Wir müssen zeigen, dass a und b Vielfache von 3 sind.

Dazu treffen wir eine Fallunterscheidung über den Grad von x:

1. $[\mathbb{Q}(x) : \mathbb{Q}] = 1$. Dann muss b Null sein (und ist somit ein Vielfaches von 3). Das Minimalpolynom von x ist daher $X - \frac{1}{3}a$ und besitzt nach Voraussetzung nur ganzzahlige Koeffizienten. Daher gilt $a/3 \in \mathbb{Z}$, also ist auch a in der Tat ein Vielfaches von 3.
2. $[\mathbb{Q}(x) : \mathbb{Q}] = 2$. Durch Umstellen und Quadrieren erhält man die Polynomgleichung
$$x^2 - \frac{1}{3}(2a + b)x + \frac{1}{9}(a^2 + ab + b^2) = 0$$
für x. Das Polynom $X^2 - \frac{1}{3}(2a + b)X + \frac{1}{9}(a^2 + ab + b^2)$ muss daher das Minimalpolynom von x sein, also erhalten wir, dass
$$3 \mid 2a + b \quad \text{und} \quad 9 \mid a^2 + ab + b^2.$$
Schreiben wir $a = 3\tilde{a} + r$ und $b = 3\tilde{b} + s$ für gewisse Reste $r, s \in \{0, 1, 2\}$, erhalten wir
$$3 \mid 2r + s \quad \text{und} \quad 9 \mid r^2 + rs + s^2.$$

Wir können nun einfach alle Möglichkeiten für r und s ausprobieren (oder uns klüger anstellen)...

r	s	$2r+s$	r^2+rs+s^2
0	0	0	0
0	1	1	1
0	2	2	4
1	0	2	1
1	1	3	3
1	2	4	7
2	0	4	4
2	1	5	7
2	2	6	12

... und sehen, dass der einzige Fall, der die Teilbarkeitsbedingung erfüllt, $r = s = 0$ ist. Das war zu zeigen.

Damit ist bewiesen, dass $(1, (1+z)/2)$ eine Ganzheitsbasis von $\mathcal{O}_K$ ist.

Hier noch, was passiert wäre, wenn man nicht erkannt hätte, dass $1, z$ keine Ganzheitsbasis sein konnte. Die Diskriminante hätte sich zu -12 ergeben. Für ein beliebiges $x \in \mathcal{O}_K$ hätte es daher ganze Zahlen $a, b \in \mathbb{Z}$ mit $x = \frac{1}{12}a + \frac{1}{12}b\sqrt{-3}$ gegeben, und man hätte versuchen müssen, zu zeigen, dass a und b Vielfache von 12 sind.

Wie oben hätte man dann eine Fallunterscheidung über den Grad von x getroffen, der erste Fall hätte auch noch funktioniert. Im zweiten Fall wäre man auf das Minimalpolynom

$$X^2 - \frac{1}{6}aX + \frac{1}{144}(a^2 + 3b^2)$$

gekommen und hätte daher folgern können, dass

$$6 \mid a \quad \text{und} \quad 144 \mid a^2 + 3b^2.$$

Beim Versuch zu zeigen, dass aus dieser Teilbarkeitsbedingung aber schon folgt, dass a und b Vielfache von 12 sind, wäre man aber gescheitert: Beispielsweise erfüllt $(a, b) = (6, 6)$ auch die Bedingung. Die zugehörige Zahl x ist

$$x = \frac{1}{12}6 + \frac{1}{12}6\sqrt{-3} = \frac{1+\sqrt{-3}}{2},$$

nimmt man diese anstelle von z als zweites Basiselement, wird man zu einer neuen Vermutung über die Ganzheitsbasis geleitet (unserer zweiten Vermutung), mit der man das Verfahren wiederholen kann.

Allgemeines Verfahren zur Bestimmung einer Ganzheitsbasis

Das Beispiel zeigt, dass man folgendes Verfahren zur Bestimmung einer Ganzheitsbasis verwenden kann:

1. Beginne mit einer $\mathbb{Q}$-Basis $b_1, \ldots, b_n$ von K, die aus Elementen von $\mathcal{O}_K$ besteht.
2. Berechne ihre Diskriminante $d := D(b_1, \ldots, b_n)$.

3. Versuche zu zeigen, dass $\mathcal{O}_K \cap \left(\mathbb{Z}\frac{1}{d}b_1 + \cdots + \mathbb{Z}\frac{1}{d}b_n\right) \subseteq \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n$.

   Nehme dazu ein beliebiges $x = \frac{1}{d}a_1b_1 + \cdots + \frac{1}{d}a_nb_n$ mit ganzen Zahlen $a_1, \ldots, a_n$ und $x \in \mathcal{O}_K$. Treffe eine Fallunterscheidung über den Grad von x und bestimme in jedem Fall sein Minimalpolynom.

   Versuche dann aus dem Wissen, dass die Koeffizienten des Minimalpolynoms ganze Zahlen sind, zu zeigen, dass die a_i jeweils Vielfache von d sind. Hilfreich ist es dabei, ohne Einschränkung der Allgemeinheit anzunehmen, dass jedes a_i schon in der Menge $\{0, 1, \ldots, |d| - 1\}$ liegt. (Das haben wir oben über die Division mit Rest erreicht.)

4. War der Versuch erfolgreich? Dann ist $b_1, \ldots, b_n$ eine Ganzheitsbasis von $\mathcal{O}_K$.

   Sonst kann man aus dem Fehlschlag ein Element aus $\mathcal{O}_K$ extrahieren, welches keine $\mathbb{Z}$-Linearkombination der Basis $b_1, \ldots, b_n$ ist; fügt man dieses in die Basis ein (und entfernt dafür ein anderes Basiselement), kann man das Verfahren ab Schritt 2 für die neue Basis wiederholen.

In der Praxis hilfreich ist es, gleich zu Beginn auszuloten, ob Zahlen wie $(1 + z)/2$ ganz-algebraisch sind und so zu einer besseren Vermutung über die Ganzheitsbasis zu gelangen. Das spart Zeit.

Siehe auch

- `http://en.wikipedia.org/wiki/Ring%20of%20integers`
- `http://planetmath.org/encyclopedia/ExamplesOfRingOfIntegersOfANumberField.html`
- `http://www.ucl.ac.uk/~ucahmki/courses/ant/integral.pdf`
- `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/nopowerbasis.pdf`