Algebraische Zahlentheorie: [MTH-1483]
Vorlesungsskript

Ilia Pirashvili

WS 2021/2022
Universität Augsburg

Inhaltsverzeichnis

1 Hintergrundmaterial **3**
1.1 Ringe und Ideale . . . 3
1.1.1 Ringe und Ringhomomorphismen . . . 3
1.1.2 Ideale . . . 5
1.1.3 Hauptideale . . . 7
1.1.4 Primideale . . . 11
1.1.5 Quotientenringe . . . 12
1.1.6 Der Kern . . . 12
1.2 Lokalisation . . . 14
1.2.1 Lokalisation von Monoiden . . . 14
1.2.2 Lokalisation von Ringen . . . 16
1.3 Körpererweiterungen . . . 20
1.3.1 Algebraische Elemente . . . 20
1.3.2 Normierte Polynome . . . 21
1.3.3 Irreduzible, reduzible und invertierbare Elemente . . . 21
1.3.4 Grad einer Körpererweiterung . . . 23
1.4 Polynome über $\mathbb{Z}[X], \mathbb{Q}[X]$ und das Lemma von Gauß . . . 29
1.4.1 Primitive Polynome . . . 29
1.4.2 Weitere Tricks für Polynomzerlegungen . . . 30
1.5 Symmetrische Polynome . . . 34
1.5.1 Der Satz von Newton . . . 35

2 Algebraische Zahlenkörper **41**
2.1 Körpereinbettungen . . . 41
2.2 Die Norm, die Spur und die Diskriminante . . . 44
2.2.1 Die Standardbasis . . . 46
2.3 Ganzalgebraische Zahlenringe . . . 51
2.4 Ganzheitsbasis . . . 56
2.4.1 Algorithmus zum finden einer Ganzheitsbasis . . . 57
2.4.2 Ganzheitsbasen von quadratischen Körpern . . . 60
2.4.3 Ganzheitsbasen von kubischen Körpern . . . 61
2.4.4 Norm und Ganzheit in Eisenstein Körpern . . . 67
2.4.5 Ganzheitsbasen von Kreisteilungskörper/Zyklotomische Körper . . . 69

3 Faktorisierung in $\mathfrak{o}_K$ **73**
3.1 Eindeutige faktorisierung von Idealen . . . 75
3.2 Noetherheit von $\mathfrak{o}_K$ . . . 76
3.3 Bruchideale . . . 80
3.4 Norm von Idealen . . . 87
3.4.1 Norm von Primidealen . . . 91
3.5 Dedekinds Primfaktorzerlegung . . . 95
3.5.1 Algorithmus für die Zerlegung in Maximalideale . . . 98
3.6 Idealklassengruppe . . . 101
3.6.1 Methode zum berechnen der Idealklassengruppe . . . 103
3.7 Minkowski-Schranke . . . 108
3.7.1 Gittertheorie und der Minkowskische Gitterpunktsatz . . . 108
3.7.2 Das Lemma von Messy . . . 109
.0.3 Vorlesungsversion der Endlichkeit der Idealklassengruppe . . . 115

1 Hintergrundmaterial

1.1 Ringe und Ideale

1.1.1 Ringe und Ringhomomorphismen

Definition 1.1.1. Ein Monoid ist eine Menge M, zusammen mit einer binären Verknüpfung $\cdot : M \times M \to M$ und ein ausgewähltes Element $1 \in M$, so dass für alle $a, b, c \in M$ gilt

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- $1 \cdot a = a$.

Definition 1.1.2. Ein *Ring* R ist eine Menge mit 2 binären Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$, so dass für all $a, b, c \in R$ gilt:

1. R ist eine *abelsche Gruppe* unter der Addition:
   - $(a + b) + c = a + (b + c)$ (Assoziativität)
   - $a + b = b + a$ (Kommutativität)
   - Es gibt ein Element $0 \in R$, so dass $a + 0 = a$ (Additive Identität)
   - Für jeden $a \in R$ gibt es ein $-a \in R$, so dass $a + (-a) = 0$. (Additives Inverse)
2. R ist ein *Monoid* unter der Multiplikation:
   - $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativität)
   - Es gibt ein Element $1 \in R$, so dass $a1 = a$ (Multiplikative Identität)
3. Addition und Multiplikation sind distributiv zueinander:
   - $a \cdot (b + c) = (a \cdot b) + (a \cdot d)$
   - $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Ein Ring heißt kommutativ, wenn zusätzlich $a \cdot b = b \cdot a$ gilt; also das multiplikative Monoid kommutativ ist. Von nun an und *durchgehend* in diesem Kurs, wird unter Ring ein kommutativer Ring mit 1 gemeint sein. (Bei einigen Autoren wird es nicht verlangt, dass R unter der Multiplikation ein Monoid ist, sondern nur eine Semi-Gruppe. - Das heißt, die Einheit wird nicht verlangt.) Monoide sind für uns auch immer kommutativ.

Beispiel 1.1.3. Einige Beispiele von Ringen sind $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Andere Beispiele sind $\mathbb{Z}/n\mathbb{Z}$, welche wir in kürze genauer erklären werden. Beispiele von nicht-kommutativen Ringen sind $n \times n$ Matrizen über einen kommutativen Ring.

Definition 1.1.4. Sein R, S zwei Ringe und $f : R \to S$ eine Abbildung. Dann heißt f ein *Ringhomomorphismus* wenn:

1. Es ein *Gruppenhomomorphismus* ist
   - $f(a + b) = f(a) + f(b)$;
2. Es ein *Monoidhomomorphismus* ist
   - $f(a \cdot b) = f(a) \cdot f(b)$
   - $f(1_R) = 1_S$ (1_R und 1_S indizieren, dass es die Einheiten von R und S sind).

Man erinnere sich, dass aus einem Gruppenhomomorphismus $f(0_R) = 0_S$ folgt. Statt Ring- Gruppen- Monoidhomomorphismen werden wir öfters nur Homomorphismus sagen, wenn es klar ist, worauf wir uns beziehen. Wir werden hauptsächlich auch ab für $a \cdot b$ schreiben.

Beispiel 1.1.5. Beispiele von Ringhomomorphismen sind:

- Die Identität $\mathsf{Id}(r) = r$, $r \in R$ ist immer ein Ringhomomorphismus.
- $-1 : \mathbb{Z} \to \mathbb{Z},\ n \mapsto -n$ ist *kein!* Ringhomomorphismus, da 1 nicht auf 1 geht. - Mehr als das: Es gibt genau einen Homomorphismus $\mathbb{Z} \to R$ für jeden beliebigen Ring R, siehe Proposition 1.1.6.
- Die komplex-konjugierte Abbildung $\mathbb{C} \to \mathbb{C},\ a + bi \mapsto a - bi$ ist ein Ringhomomorphismus.
- Die Abbildungen $\mathbb{C} \to \mathbb{C}, a + bi \mapsto a^2 \pm b^2$ sind keine Ringhomomorphismen, da

$$\begin{array}{ccc} (a+bi)+(u+vi) & \longmapsto & (a^2 \pm b^2)+(u^2 \pm v^2) \\ \| & & \nparallel \\ (a+u)+(b+v)i & \longmapsto & (a^2+2au+u^2) \pm (b^2+2bv+v^2). \end{array}$$

- Die Abbildung $R \to R,\ x \mapsto x^p$ ist genau dann ein Ringhomomorphismus, wenn R die Charakteristik p hat. Es wir das *Frobeniushomomorphismus* genannt.

  Hier beachte man, dass R nicht $\mathbb{F}_p$ sein muss. Zum Beispiel hat $\mathbb{F}_4 = \mathbb{F}_2[X]/x^2 + x + 1$ auch die Charakteristik 2.

  Wenn R nicht die Charakteristik p hat, dann ist $x \mapsto x^p$ kein Ringhomomorphismus, da sonst $(a+b)^p \neq a^p + b^p$.

Proposition 1.1.6. *Sei R ein Ring und $\mathbb{Z}$ das Ring der ganzen Zahlen. Es gibt genau einen Ringhomomorphismus $\mathbb{Z} \to R$.*

Beweis. Aufgabe 1 □

Definition 1.1.7. Ein Ring heißt *Körper*, wenn

- $0 \neq 1$ gilt;
- Es zu jedem $0 \neq a \in R$, ein $b \in R$ gibt, so dass $ab = 1$.

Beispiele von Körpern sind $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z}$, mit $p \in \mathbb{Z}$ eine Primzahl.

Für einen Ring R wird mir $R[X]$ das *Polynomring*, bzw. *Ring der Polynome* in der Variable x gekennzeichnet, mit Koeffizienten in R. In anderen Worten,

$$R[X] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R, n \in \mathbb{N}\}.$$

Es ist klar, das dies wieder ein Ring ist. Ein Koeffizient heißt *vom Grad m*, wenn es vor x^m steht. Das Koeffizient des höchsten Grades (welcher nicht null ist) wird *Leitkoeffizient* genannt. Der *Grad* $\mathsf{grad} f$ eines Polynoms $f(x)$ ist der Grad dessen Leitkoeffizients. In anderen Worten, der Grad $\mathsf{grad}(f)$ eines Polynoms $f = f(x) = a_0 + a_1 x + \cdots a_n x^n \in R[X]$ ist der höchste $n \in N$, wessen Koeffizient a_n ungleich null ist. Der Grad des Nullpolynoms ($a \mapsto 0\ \forall a \in R$) wird nach Vereinbarung oft als $-\infty$ gesetzt. Ein Polynom ist genau dann null, wenn dessen Leitkoeffizient null ist. Ein Polynom heißt eine *Konstante*, wenn dessen Grad null oder $-\infty$ ist.

Man erinnere sich, dass ein *Integritätsbereich* oder *Integritätsring* ein Ring ist, wo für alle $a, b \in R$ mit $ab = 0$ folgt $a = 0$ oder $b = 0$. In anderen Worten, aus $a \neq 0, b \neq 0$ folgt $ab \neq 0$. Es gilt:

Lemma 1.1.8. *Sei R ein Integritätsbereich. Das Polynomring $R[X]$ ist ein Integritätsbereich.*

Beweis. Sein $f(x)$ und $g(x)$ ungleich null und $a_n \neq 0$, $b_n \neq 0$ ihre zugehörigen Leitkoeffizienten. Wir haben $a_n b_n \neq 0$ da R ein Integritätsbereich ist. Es folgt, dass $fg = fg(x) = f(x)g(x) \neq 0$, da $a_n b_n$ dessen Leitkoeffizient ist. □

Spezifisch, wenn K ein Körper ist, dann ist $K[X]$ immer ein Integritätsbereich. $\mathbb{Z}$ is auch ein bekanntes Beispiel eines Integritätsringes. Beispiele von Nichtintegritätsringen sind $\mathbb{Z}/n\mathbb{Z}$, wenn n keine Primzahl ist, wie wir es in kürze sehen werden. Allgemeiner ist das Produkt von Ringen nie ein Integritätsbereich, es sei den eines der Ringe ist das triviale Ring mit einem Element. Spezifisch ist das Produkt von Körpern nie ein Körper.

Lemma 1.1.9. *Sei R ein Integritätsbereich, $R[X]$ das Polynomring über R und $f \neq 0, g \neq 0 \in R[X]$ Polynome ungleich null. Es gilt*

i) $\mathsf{grad}(fg) = \mathsf{grad}(f) + \mathsf{grad}(g)$.

ii) $f(x)|g(x) \Rightarrow \mathsf{grad}(f) \leq \mathsf{grad}(g)$.

iii) $\mathsf{grad}(f+g) \leq \max(\mathsf{grad}(f), \mathsf{grad}(g))$.

iv) $\mathsf{grad}(f) = 0 \iff f(x) = a$, *mit* $a \in R \setminus \{0\}$.

Beweis. i) Sein

$$f = f(x) = a_0 + a_1 X + \ldots + a_n X^n \in R[X]$$

und

$$g = g(x) = b_0 + b_1 X + \ldots + b_m X^m \in K[X]$$

mit $a_n \neq 0, b_m \neq 0$. Da R ein Integritätsbereich ist, folgt dass $a_n b_m \neq 0$. Da für jeden Ring R gilt

$$f(x)g(x) = a_0 b_0 + c_1 X + \cdots + c_{n+m-1} X^{n+m-1} + a_n b_m X^{n+m},$$

folgt das Resultat.
ii)+ iii)+ iv): Aufgabe. □

Natürlich kann man auch multiple Variablen haben: $R[X_1, \ldots, X_n]$, wobei n hier nicht endlich sein muss.

1.1.2 Ideale

Definition 1.1.10. Eine Teilmenge $I \subseteq R$ heißt *Ideal*, wenn es für jeden $a, b \in I, r \in R$ gilt:

- $0 \in I$,
- $a + b \in I$,
- $ra \in I$.

Die Menge der Ideale von R werden wir mit $\mathcal{I}(R)$, oder einfach $\mathcal{I}$, bezeichnen. Wenn man mit Modulen vertraut ist, dann kann man sehen, dass Ideale äquivalent zu Unter- bzw. Teilmodulen von R sind.

Lemma 1.1.11. *Der Schnitt von Idealen ist wieder ein Ideal.*

Beweis. Sei J eine Menge und I_j eine Kollektion von Idealen, indexiert durch J.

- $0 \in I_j$, $\forall j \in J \Rightarrow 0 \in \bigcap_{j \in J} I_j$ (wenn 0 in jedem ist, so ist es auch im Schnitt).
- Sein $a, b \in \bigcap_{j \in J} I_j$. Daher, $a, b \in I_j$ für jeden $j \in J$. Da jedes I_j ein Ideal ist, gilt $a \cap b \in I_j$ für jeden $j \in J$ und daher, $a \cap b \in \bigcap_{j \in J} I_j$.
- Sei $r \in R$ und $a \in \bigcap_{j \in J} I_j$. Dann ist $a \in I_j$ für jeden $j \in J$ und so ist $ra \in I_j$, $j \in j$. Es folgt $ra \in \bigcap_{j \in J} I_j$.

□

Sei $A \subseteq R$ eine Teilmenge von R. Dann kann man von einem Ideal *erzeugt* durch A sprechen, bezeichnet (A), indem man den Schnitt aller Ideale nimmt, die A enthalten.

Lemma 1.1.12. *Sei $I \subseteq R$ ein Ideal und $A \subseteq I$ eine Teilmenge. Dann gilt $(A) \subseteq I$.*

Beweis. Dies is klar. (A) ist der Schnitt aller Ideale, die ganz A enthalten. Das heißt, es ist in jedem Ideal drin, die A enthält. Bei Definition ist I eines dieser geschnittenen Ideale. □

Korollar 1.1.13. *Sei $u \in R^*$ eine Einheit in R. Aus $u \in I$ folgt $I = (1) = R$.*

Beweis. Bei Definition einer Einheit gibt es ein $v \in R$ mit $uv = 1$. Man setze in der dritten Eigenschaft bei der Definition eines Ideals $r = v$ und $a = u$ ein. Es folgt, dass $1 \in I$. Mit der selben Eigenschaft ist nun ein beliebiges Element im Ideal. □

Ein Ideal I heißt *endlich Erzeugt* wenn es eine endliche Menge $A := \{a_1, \dots, a_n\}$ gibt, mit $(A) := (a_1, \dots, a_n) = I$.

Lemma 1.1.14. *Sei $I = (a_1, \dots, a_n)$ endlich erzeugt. Es gilt:*

$$(a_1, \dots, a_n) = \left\{ \sum_{i=1}^{n} r_i a_i \right\}, \quad \text{wobei die } r_i \text{ alle Elemente von } R \text{ durchlaufen.}$$

Beweis. Zuerst bemerken wir, dass die rechte Seite ein Ideal ist. Als solches gilt $\mathsf{LS} \subseteq \mathsf{RS}$, da die a_i's natürlich in der rechten Seite liegen und bei Definition, die linke Seite das kleinste Ideal ist, in der die a_i's liegen.

Auf der anderen Seite muss in jedes Ideal in der a_i liegt, auch $r_i a_i$ liegen, für einen beliebigen $r_i \in R$. Des weiteren muss auch all deren Summen darin liegen, da ein Ideal unter der Summe abgeschlossen ist. Es folgt, dass die rechte Seite in der linken liegt. □

Dies gilt auch für nicht-endlich erzeugte Ideale, da muss man allerdings bei der Summe beachten, dass *fast alle* Summanden null sind. Für diesen Kurs reichen endlich erzeugte Ideale aus.

Bemerkung 1.1.15. *Fast alle* ist ein mathematisch rigoroser Begriff, das *alle außer endlich vielen* bedeutet.

Lemma 1.1.16. *Sei $f : R \to S$ ein Ringhomomorphismus und $I \subseteq S$ ein Ideal.*

(i) Das Urbild $f^{-1}(I) \subseteq R$ ist ein Ideal von R.

(ii) Wenn $f : R \to S$ surjektiv ist, dann ist $f(I) \subseteq S$ ein Ideal von S.

Beweis. (i) Aufgabe 3 und (ii) Aufgabe 4. □

Bemerkung 1.1.17. Auf der Menge der Ideale $\mathcal{I}(R)$ haben wir viele nette Verknüpfungen. Für $I, J \subseteq R$ Ideale eines Ringes R sind

i) $I \cap J := \{r \in R \mid r \in I \text{ und } r \in J\}$,

ii) $IJ = I \times J := (xy \mid x \in I, y \in J) = \{ \sum_{x \in I, y \in J} r_{x,y} xy \mid r_{x,y} \in R\}$ und

iii) $I + J := (x + y \mid x \in I, y \in J) = \{ \sum_{x \in I, y \in J} r_{x,y}(x + y) \mid r_{x,y} \in R\}$

wieder Ideale von R. Bei den letzten zwei nehmen wir nur endliche Summen.

1.1.3 Hauptideale

Ein Ideal I heißt *Hauptideal* wenn es einen Element $a \in I$ gibt, mit $I = (a)$. Hauptideale sind besonders schön, da $(a) = \{ra \mid r \in R\}$ einfach nur die vielfachen von a sind.

Beispiel 1.1.18.

- Sei $\mathbb{Z}$ unser Ring. Das Hauptideal erzeugt mit $2 \in \mathbb{Z}$ ist

$$(2) = \{\ldots, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\}.$$

- Sei $R = \mathbb{Z}[X]$ das Ring der Polynome mit Koeffizienten in den ganzen Zahlen.
  - Das Hauptideal erzeugt mit $x \in \mathbb{Z}[X]$ ist

$$(x) = \{x, x^2, \ldots, 2x, 3x, \ldots, 9x + 7x^2 + 5x^{19}, \ldots\}.$$

    Also, alle Polynome die durch das Polynom x teilbar sind.
  - Das Hauptideal erzeugt mit $x^2 + 17 \in \mathbb{Z}[X]$ ist

$$(x^2 + 17) = \{x^2 + 17, +2(x^2 + 17), \ldots, x(x^2 + 17), \ldots, (x^3 + 2x^4)(x^2 + 17), \ldots\}.$$

In einem Ring R sagen wir *a teilt b*, wenn es ein Element $c \in R$ gibt, mit $ac = b$. Wir benutzen die Notation $a \mid b$. Für Hauptideale gilt:

Lemma 1.1.19. *Sei R ein Ring, und $a, b \in R$ Elemente. Wir haben*

$$a \mid b \iff (b) \subseteq (a).$$

Beweis. Nimm an, dass $a \mid b$. Das heißt $\exists c \in R$, so dass $ac = b$. Sei $x \in (b) = \{rb \mid r \in R\}$. Daher,

$$x = rb = r(ac) = (rc)a \in (a) = \{ra \mid r \in R\}.$$

□

Korollar 1.1.20. *Sei $u \in R$ eine Einheit und $(a) \subseteq R$ ein Ideal. Dann gilt*

$$(a) = (ua).$$

Beweis. Aufgabe 5. □

Ein Hauptideal ist nicht immer sofort erkennbar, denn es könnte sein, dass man "zu viele" Erzeuger genommen hat: z.B., $(R) = (1)$ für jeden Ring. Ein anderes Beispiel ist das folgende:

Beispiel 1.1.21. Man betrachte das Ideal $(4, 6) \subseteq \mathbb{Z}$. Laut Lemma 1.1.14 gilt

$$(4, 6) = 4n + 6m, \quad n, m \in \mathbb{Z}.$$

Da $2 = 4 \cdot (-1) + 6 \cdot 1$ folgt laut Lemma 1.1.12, dass $(2) \subseteq (4, 6)$. Auf der anderen Seite ist $(2) = n \cdot 2$, also die geraden Zahlen. Da $4n + 6m = 2(2n + 3m)$ gilt, folgt, dass $(4, 6) \subseteq (2)$. Daher ist

$$(4, 6) = (2).$$

Dies stimmt allgemeiner:

Proposition 1.1.22. *Sei $(n, m) \subseteq \mathbb{Z}$ ein ideal und $\mathtt{ggt}(n, m)$ der größte gemeinsame Teiler von $n, m \in \mathbb{Z}$. Es gilt*

$$(n, m) = (\mathtt{ggt}(n, m)).$$

Beweis. Wir wissen, dass

$$(n, m) \subseteq (\mathtt{ggt}(n, m))$$

ist, da n ein vielfaches von $\mathtt{ggt}(n, m)$ ist und daher $n \in (\mathtt{ggt}(n, m))$. Ebenso mit m. Auf der anderen Seite, benutzen wir das euklidische Algorithmus (siehe unten) un zu schlussfolgern, dass $\mathtt{ggt}(n, m) = an + bm$, mit $a, b \in \mathbb{Z}$ und daher ist $\mathtt{ggt}(n, m) \in (n, m)$. □

Wir erinnern uns kurz an dem euklidischen Algorithmus. Die Idee ist es, den größten gemeinsamen Teiler zweier Zahlen zu finden. Dazu betrachten wir zwei wichtige Beispiele:

Beispiel 1.1.23.

- Sein $147, 15 \in \mathbb{Z}$ zwei ganze Zahlen. Wir betrachten

$$\begin{aligned} 147 &= 15 \cdot 9 + 12 \\ 15 &= 12 \cdot 1 + 3 \\ 12 &= 3 \cdot 4 + 0 \end{aligned}$$

  Daher ist 3 der größte gemeinsame Teiler. Man beachte auch, dass $|12| < |15|$ und $|3| < |12|$ streng kleiner sind. Wir müssen hier nicht "klug" sein und den großen durch den kleinen Teilen. Wir hätten auch andersrum teilen können:

$$\begin{aligned} 15 &= 147 \cdot 1 + (-132) \\ 147 &= (-132) \cdot (-1) + 15 \\ -132 &= 15 \cdot (-9) + 3 \\ 15 &= 3 \cdot 5 + 0 \end{aligned}$$

- Sein $f(x) = x^3 + 2x^2 + 4, g(x) = 4x + 9$ zwei Polynome in $\mathbb{Q}[X]$. Wir teilen f durch g, genau wie bei den ganzen Zahlen:

$$\begin{aligned} x^3 + 2x^2 + 4 &= (4x + 9)\left(\frac{1}{4}x^2 - \frac{1}{16}x + \frac{9}{64}\right) + \frac{175}{64} \\ (4x + 9) &= \frac{175}{64}\left(\frac{256}{175}x + \frac{576}{175}\right) + 0 \end{aligned}$$

In beiden Fällen sehen wir, dass für jedes Paar von Elementen $r \neq 0, s \neq 0$, wir $r = sa + b$ haben, wobei $|b| < |s|$. Im ersten Fall ist $|\cdot|$ die Norm, im zweiten Fall ist es der Grad. Im allgemeinen reicht es aus, wenn auf dem gegebenen Ring eine so genannte *euklidische Funktion* gegeben ist. Solche Ringe nennt man *euklidische Ringe*.

Definition 1.1.24. Ein Ring R heißt *Hauptidealring* wenn jedes Ideal $I \subseteq R$ ein Hauptideal ist.

Euklidische Ringe sind immer Hauptidealringe. Uns reichen aber $K[X]$ (K Körper) und $\mathbb{Z}[X]$ aus.

Proposition 1.1.25. *Der Ring $\mathbb{Z}$ ist ein Hauptidealring.*

Beweis. Aufgabe 6. □

Proposition 1.1.26. *Sei K ein Körper, dann ist $K[X]$ ein Hauptidealring.*

Beweis. Sei $(1) \neq I \neq (0)$ ein Ideal und $0 \neq f(x) \in I$ ein Polynom mit kleinstmöglichem Grad, so dass $\mathsf{grad}(f) \geq 1$. Wir können so einen Polynom finden, da $I \neq (1)$, sieh Lemma 1.1.13. Wir wollen zeigen, dass jedes Element in I ein vielfaches von $f(x)$ ist. In anderen Worten, dass $I = (f)$.

Sei $g(x) \in I$. Der euklidische Algorithmus besagt, dass es Elemente $h(x), r(x) \in K[X]$ gibt, mit

$$g(x) = f(x)h(x) + r(x)$$

und $\mathsf{grad}(r) < \mathsf{grad}(f)$. Es folgt,

$$r(x) = g(x) - f(x)h(x) \in I,$$

da $f(x), g(x) \in I$. Da $f(x)$ den kleinstmöglichen streng-positiven Grad hatte, folgt $r(x) = c$, wobei c eine konstante Funktion in $K[X]$ ist ($c \in K$). Da von $c \neq 0 \iff c \in K^\times$ folgt $I = (1)$ (Lemma 1.1.13), haben wir $r(x) = c = 0$ und $g(x) = f(x)h(x)$, also $g(x) \in (f)$. □

Definition 1.1.27. Sei R ein Ring und $a, b \in R$ Elemente mit $a \neq 0, b \neq 0$.

- Wir nennen $d = \mathtt{gt}(a,b) \in R$ einen *gemeinsamen Teiler*, wenn es $u, v \in R$ gibt, mit $a = ud$ und $b = vd$.
- Wir nennen $d = \mathtt{ggt}(a,b) \in R$ den *größten gemeinsamen Teiler*, wenn für jeden gemeinsamem Teiler $d' \in R$ von a, b gilt $d' \mid d$.

Nicht jedes Ring hat größte gemeinsame Teiler. Wir werden Gegenbeispiele in kürze kennenlernen. Sieh Beispiel **??**. Auch wenn es existiert, ist der ggt nicht ganz Eindeutig, nur bis auf Multiplikation mit einem invertierbaren Element. In einigen Fällen aber, kann man es ganz eindeutig machen, indem man zusätzliche Bedingen verlangt. Z.B., in $\mathbb{Z}$ reicht es aus zu verlangen, dass der ggt positiv sein muss. In $K[X]$ reicht es aus, wenn der ggt zusätzlich normiert ist.

Proposition 1.1.28. *Sei K ein Körper und $K[X]$ das dazugehörige Polynomring. Sein $f, g \in K[X]$. Dann existiert $\mathtt{ggt}(f,g)$, der größte gemeinsame Teiler von f und g und es gilt die Gleichung der Ideale*

$$(f,g) = (\mathtt{ggt}(f,g)).$$

Beweis. Laut Proposition 1.1.26 gibt es ein $h(x) \in K[X]$, so dass

$$(f,g) = (h).$$

Gleichheit besagt, dass $\subseteq$ sowohl auch $\supseteq$ gilt. Von $\subseteq$ folgt, dass es $a(x), b(x) \in K[X]$ gibt, mit $f = ah$ und $g = bh$. In anderen Worten, dass h ein gemeinsamer Teiler von f und g ist.

Sei nun $k \in K[X]$ ein beliebiger gemeinsamer Teiler von f und g. Also, $\exists c, d \in K[X]$ mit $f = ck$ und $g = dk$. Die andere Seite $\supseteq$ besagt, dass $h \in (f,g)$. Also, dass es $u, v \in K[X]$ gibt, mit $h = uf + vg$. Nach Einsetzen haben wir

$$h = uf + vg = uck + vdk = [uc + vd]k.$$

Daher ist k ein Teiler von h und somit ist h der größte gemeinsame Teiler von f und g. □

Korollar 1.1.29. *Sei K ein Körper und $f, g \in K[X]$. Dann gibt es Polynome $u(x), v(x) \in K[X]$, so dass*

$$\mathtt{ggt}(f,g) = uf + vg.$$

Beispiel 1.1.30. Sei $I \subseteq R$ ein Hauptideal. Man könnte meinen, dass in einem Hauptideal genau ein irreduzibles Element gibt. Dies ist jedoch nicht ganz richtig. Sei $I = (0) = \{0\}$. Dann ist kein irreduzibles Element in (0). Auf der anderen Seite, wenn $I = (u) = (1)$, $u \in R^*$ Einheit, dann kann es sehr viele irreduzible Elemente in (1) geben. (Sogar bei $R = \mathbb{Z}$ gibt es unendlich viele).

Sei $r \in R$ ein irreduzibles Element. Dann hat $I = (r)$ genau ein irreduzibles Element, bis auf Einheiten, nämlich r selbst. Wenn $a \in R$ jedoch reduzibel ist, also das Produkt von 2 irreduziblen Elementen, dann hat (a) kein irreduzibles Element.

Beispiel 1.1.31. Nicht jedes Ring ist ein Hauptidealring. Zum Beispiel, $\mathbb{Z}[X]$ ist schon kein Hauptidealring. Man betrachte dafür $(2, x) \subseteq \mathbb{Z}$. Es gilt

$$(2,x) = \{2, 4, -10, \ldots, x, x^2, x^7 + 3x^2, \ldots, x+2, 3x^2 + 10 \ldots\}.$$

Da 2 und x schon irreduzibel sind, können die nicht beide als das Vielfache eines einzigen Elements sein. Daher kann es kein Hauptideal sein. Im Gegensatz zum Hauptideal können wir hier schon unendlich viele irreduzible Elemente haben. Z.B., $x + 2$ ist ein weiteres Irreduzibles Element, wie auch $x + 4, x + 6$ etc.

Es ist klar, dass $(1) = R \subseteq R$ und $(0) = \{0\} \subseteq R$ für jeden Ring Ideale sind. Des weiteren gilt $(0) = (1)$ genau dann, wenn $R = \{0\}$ der Nullring ist.

Lemma 1.1.32. *Ein Ring R ist genau dann ein Körper, wenn es nur die kanonischen Ideale $I = (0) = \{0\}$ und $I = (1) = R$ hat und zusätzlich $(1) \neq (0)$ gilt.*

Beweis. Zuerst, nimm an, dass R ein Körper ist und sei $I \subseteq K$ ein Ideal. $0 \in I$ bei Definition. Wenn es sonst kein Element hat gilt $I = \{0\}$. Sei daher $0 \neq x \in I$. Da K ein Körper ist folgt, dass x eine Einheit ist. Korollar 1.1.13 und die Tatsache, dass $0 \neq 1$ in einem Körper beendet nun den Beweis. □

Aufgaben

Aufgaben 1

Aufgabe 1 (1 Punkt). Sei R ein Ring und $\mathbb{Z}$ das Ring der ganzen Zahlen. Zeige, dass es genau einen Ringhomomorphismus $\mathbb{Z} \to R$ gibt.

Aufgabe 2 (5 Punkte (insgesamt)). Sei X eine Menge und $\mathfrak{P}(X)$ die Menge der Teilmengen von X.

- (2 Teilpunkte) Zeige, dass

$$A + B := A \cup B \setminus A \cap B \quad \text{und} \quad AB := A \cap B$$

  eine Ringstruktur auf $\mathfrak{P}(X)$ definiert.

  – Überzeugt euch, dass für ein beliebiges Element A, $2A = 0$ in diesem Ring.

- (3 Teilpunkte) Ist es möglich, mithilfe von Teilmengen einer Menge X, einen Ring der Charakteristik 3 zu definieren?

Definition. Zur Erinnerung, ein Ideal $\mathfrak{p} \subseteq R$ heißt *prim* wenn aus $ab \in \mathfrak{p}$ folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

Aufgabe 3 (2 Punkt (insgesamt)). Sei $f : R \to S$ ein Ringhomomorphismus und $I \subseteq S$ ein Ideal.

- (1 Teilpunkt) Beweis, dass das Uhrbild $f^{-1}(I) \subseteq R$ von I ein Ideal von R ist.
- (1 Teilpunkt) Sei $I = \mathfrak{p}$ zusätzlich prim. Zeige, dass $f^{-1}(\mathfrak{p})$ auch prim ist.

Aufgabe 4 (1 Punkt). Sei $f : R \to S$ ein surjektiver Ringhomomorphismus und $I \subseteq R$ ein Ideal. Beweise, dass $f(I) \subseteq S$ ein Ideal von S ist.

Aufgabe 5 (1 Punkt). Sei $u \in R$ eine Einheit von R und $I \subseteq R$ ein Ideal. Zeige, dass

$$I = (u)I.$$

Aufgabe 6 (2 Punkte). Beweise direkt, dass $\mathbb{Z}$ ein Hauptidealring ist.

Aufgabe 7 (2 Punkte). Sei $2 \leq p \in \mathbb{Z}$. Zeige, dass das Ideal

$$(p, x) \subseteq \mathbb{Z}[X]$$

kein Hauptideal ist.

Aufgabe 8 (2 Punkte). Bestimme, ob das Ideal $(X^2+9X+18, X^3+9X^2-54) \subseteq \mathbb{Z}[X]$ ein Hauptideal ist.

1.1.4 Primideale

Wir haben gesehen, dass Ideale von $\mathbb{Z}$ alle von der Form (n) sind. Des weiteren gilt: $(n) = (m)$ genau dann wenn $n = m$ oder $n = -m$. Das heiß, Ideale "verallgemeinern" Zahlen (bzw. Elemente eines Ringes), bis auf dem Vorzeichen. Es gibt aber eine ganz besonders schöne Teilmenge von Zahlen, nämlich die Primzahlen. Primideale sind dessen "Verallgemeinerung".

Definition 1.1.33. Ein Ideal $\mathfrak{p} \subseteq R$ heißt *prim* wenn aus $ab \in \mathfrak{p}$ folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

Lemma 1.1.34. *Ein Ideal $\mathfrak{p} \subseteq R$ ist genau dann prim, wenn aus $IJ \subseteq \mathfrak{p}$, $I, J \subseteq R$ Ideale, folgt $I \subseteq \mathfrak{p}$ oder $J \subseteq \mathfrak{p}$.*

Beweis. Nehme an, dass $\mathfrak{p}$ prim ist, $IJ \subseteq \mathfrak{p}$ und $J \nsubseteq \mathfrak{p}$. Daher, es gibt ein $x \in J \setminus \mathfrak{p}$. Bei Definition des Produkts von Idealen gilt für jeden $y \in I$, dass $xy \in IJ \subseteq \mathfrak{p}$. Da $xy \in \mathfrak{p}$, $x \notin \mathfrak{p}$ und $\mathfrak{p}$ prim ist, folgt $y \in \mathfrak{p}$. Daher $I \subseteq \mathfrak{p}$.

Sei nun die die Bedingung des Lemmas erfüllt. Wir wollen beweisen, dass $\mathfrak{p}$ prim ist. Sei dazu $xy \in \mathfrak{p}$. Es folgt, dass $(xy) \subseteq \mathfrak{p}$, also $(x)(y) = (xy) \subseteq \mathfrak{p}$. Laut Annahme musst $(x) \subseteq \mathfrak{p}$ oder $(y) \subseteq \mathfrak{p}$ sein, also $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$. □

Die Menge aller Primideale eines Ringes wird mit $\mathsf{Spec}(R)$, sprich Spektrum von R, bezeichnet. Dies wird im Kurs nicht vorkommen, ist aber wie erwartet in Algebra von großer Bedeutung.

Beispiel 1.1.35. Sei unser Ring $R = \mathbb{Z}$.

- Das Ideal (2), die Menge der geraden Zahlen, ist ein Primideal. Für diese gilt natürlich, wenn $2k = ab, k \in \mathbb{Z}$, dann muss entweder a oder b eine gerade Zahl sein, daher wieder ein Element des Ideals.
- Das Ideal (4), was die Menge der vielfachen von 4 ist, ist kein Primideal, da $4 = 2 \cdot 2$ und 2 natürlich kein vielfaches von 4 ist.

Lemma 1.1.36. *Die Primideale von $\mathbb{Z}$ sind genau von der Form $\mathfrak{p} = (p)$ oder $\mathfrak{p} = (0)$, wobei $p \in \mathbb{Z}$ eine positive Primzahl ist.*

Beweis. Sei $p \in \mathbb{Z}$ eine Primzahl, $a, b \in \mathbb{Z}$ und $ab \in (p)$. Da $(p) = \{np \mid n \in \mathbb{Z}\}$, haben wir $ab = np$ für irgend ein $n \in \mathbb{Z}$. Daher, p teilt a oder p teilt b. ohne Beschränkung der Allgemeinheit (o.B.d.A), p teilt a. Das heißt, $a = kp, k \in \mathbb{Z}$ und daher $a \in (p)$.

Auf der anderen Seite, sei $\mathfrak{p} \subseteq \mathbb{Z}$ ein Primideal. Da $\mathbb{Z}$ laut Korollar 1.1.25 ein Hauptidealring ist, folgt, dass $\mathfrak{p} = (p)$ für irgendein $p \neq \pm 1 \in \mathbb{Z}$. Es darf nicht 1 oder -1 sein, da ein Primideal by Definition ungleich (1) ist. Sei $p = ab$ eine Zerlegung von p. Daher $ab \in \mathfrak{p} = (p)$. Bei der Definition eines Primideals muss, o.B.d.A $a \in \mathfrak{p} = (p)$ sein. Dies impliziert $a = kp$ für irgendein $k \in Z$. Also $p = (kp)b \Rightarrow 1 = kb \Rightarrow k = \pm 1 \Rightarrow a = \pm p \Rightarrow p$ ist eine Primzahl oder $p = 0$. □

Lemma 1.1.37. *Ein Ring R ist genau dann ein Integritätsbereich, wenn $\{0\} = (0)$ ein Primideal ist.*

Beweis. Aufgabe 9. □

Proposition 1.1.38. *Sei $f : R \to S$ ein Ringhomomorphismus und $\mathfrak{p} \subseteq S$ ein Primideal. Dann ist $f^{-1}(\mathfrak{p}) \subseteq R$ ein Primideal von R.*

Beweis. Aufgabe 3. □

Definition 1.1.39. Ein Ideal $\mathfrak{m} \subseteq R$ heißt *maximal* wenn

- für jedes Ideal $I \subseteq R$ mit $\mathfrak{m} \subseteq I$ gilt $I = R$ oder $I = \mathfrak{m}$; und
- $\mathfrak{m} \neq R$.

In anderen Worten, es darf keinen Ideal zwischen $\mathfrak{m}$ und $(1) = R$ geben. Ein Maximalideal ist nicht eindeutig. Im allgemeinen hat ein Ring viele Maximalideale.

Beispiel 1.1.40. Sei $R = \mathbb{Z}$ das Ring der ganzen Zahlen. Dann sind die Maximalideale genau von der Form $\mathfrak{m} = (p)$, wobei $p \in \mathbb{Z}$ eine Primzahl ist.

Man betrachte, dass $(0) \subseteq \mathbb{Z}$ der einzige Primideal ist, welches kein Maximalideal ist.

1.1.5 Quotientenringe

Definition 1.1.41. Sei $I \subseteq R$ ein Ideal von R. Wir definieren den *Quotientenring*

$$R/I \coloneqq \{a + I \mid a \in R\}.$$

Dies ist ein Ring, wobei die Addition und Multiplikation wie folgt definiert werden:

$$\begin{aligned}(a+I)+(b+I) &\coloneqq (a+b)+I\\ (a+I)(b+I) &\coloneqq (ab)+I\end{aligned}$$

Dies wir oft auch als *Faktorring* oder *Restklassenring* bezeichnet.

Lemma 1.1.42. *Das Quotientenring R/I ist ein Ring, daher assoziativ, kommutativ etc.*

Beweis. Aufgabe 10. □

Es gibt eine andere Art, den Quotientenring zu beschreiben, welches Hauptsächlich im Skript benutzt wird:

Definition 1.1.43 (Alternative Definition)**.** Sei $I \subseteq R$ ein Ideal von R. Wir definieren eine Relation $\sim$ auf R, oder $\sim_I$ wenn wir den Ideal andeuten wollen, wobei $a \sim b$ genau dann, wenn $a - b \in I$.

Für die *Äquivalenzklasse* von a werden wir die Notation

$$[a] \coloneqq \{r \in R \mid a \sim r\} = \{r \in R \mid a - r \in I\}$$

benutzen. Eine andere oft benutzte Notation ist $\overline{a}$. Die Äquivalenzklassen bilden einen Ring R/I, wo die Verknüpfungen wie folgt

$$[a] + [b] \coloneqq [a+b]$$
$$[a][b] \coloneqq [ab]$$

definiert werden.

Öfters, vor allem bei den Quotientenringen $\mathbb{Z}/(n)$, werden die Notationen $\mathbb{Z}/n\mathbb{Z} \coloneqq \mathbb{Z}/(n)$ und $\overline{a} \coloneqq [a]$ benutzt. Der Ring $\mathbb{Z}/(p)$ wird auch manchmal als $\mathbb{F}_p$ bezeichnet, wenn p eine Primzahl ist.

Beispiel 1.1.44 (Aufgabe). Zeige, dass $\sim_I$ eine Kongruenzrelation ist. Des weiteren, zeige, dass es mit der ursprünglichen Definition übereinstimmt.

Eine andere Art und Weise den Quotientenring zu verstehen, ist, dass wir die multiplikative Struktur in R kurzzeitig "vergessen" und es als eine Abelsche Gruppe auffassen. Das Ideal $I \subseteq R$ wird dann eine Untergruppe und wir Teilen diese so, wie wir Gruppen herkömmlich teilen. Da R Abelsch ist, ist I ein Normalteiler und so ist das Quotient R/I wieder eine Abelsche Gruppe. Da I aber etwas mehr war (also auch mit der Multiplikation von R abgestimmt), wird das Quotient zusätzlich noch ein Ring, nachdem wir uns an die Multiplikation wieder "erinnern".

Als solches wollen wir den Haupthomomorphiesatz der Gruppentheorie hier wieder einführen. Dazu führen wir den Begriff eines Kerns wieder ein. Leider wird der Kern von zwei Ringen nicht mehr ein Ring sein. (Die 1 ist (fast) nie im Kern). Den Haupthomomorphiesatz allerdings haben wir.

1.1.6 Der Kern

Sei $f : R \to S$ ein Ringhomomorphismus. Dann definieren wir den Kern $\mathsf{Ker}(f)$ von f als

$$\mathsf{Ker}(f) = \{r \in R \mid f(r) = 0 \in S\},$$

das Urbild von 0_S. Dies Stimmt mit der Definition des Kerns einer Gruppe überein.

Proposition 1.1.45. *Sei $f : R \to S$ ein Ringhomomorphismus. Das Kern $\mathsf{Ker}(f) \subseteq R$ ist ein Ideal von R.*

Beweis. Aufgabe 11. □

Proposition 1.1.46. *Sei $f : R \to S$ ein Ringhomomorphismus. Dann gibt es einen kanonischen Isomorphismus von Ringen*

$$R/\mathsf{Ker}(f) \simeq \mathsf{Bild}(f)$$

Beweis. Aufgabe 12. □

Die obigen zwei Aussagen zusammen nennt man auch den *Hauptisomorphiesatz* oder den ersten Isomorphiesatz. Das folgende wird auch öfters als den zweiten Isomorphiesatz bezeichnet.

Proposition 1.1.47. *Sei R ein Ring und $I \subseteq J \subseteq R$ Ideale von R. Es gilt*

$$R/J = (R/I)/(J/I).$$

Beweis. Aufgabe 13. □

Auch in Ringen kann der Kern benutzt werden um Injektivität zu beschreiben. Wir haben

Proposition 1.1.48. *Ein Ringhomomorphismus $f : R \to S$ ist genau dann injektiv wenn der Kern $\mathsf{Ker}(f) = (0) = \{0\}$ trivial ist.*

Beweis. Aufgabe 14. □

Proposition 1.1.49. *Sei R ein Ring.*

- *Ein Ideal $\mathfrak{p} \subseteq R$ ist genau dann prim, wenn $R/\mathfrak{p}$ ein Integritätsbereich ist.*
- *Ein Ideal $\mathfrak{p} \subseteq R$ ist genau dann maximal, wenn $R/\mathfrak{p}$ ein Körper ist.*

Beweis. i) Sei $\mathfrak{p} \subseteq R$ ein Primideal und $[a][b] \in R/\mathfrak{p}$ mit $[a][b] = [ab] = 0$. Bei Definition 1.1.43 folgt $ab \in \mathfrak{p}$. Da $\mathfrak{p}$ prim ist, folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. In anderen Worten, $[a] = 0$ oder $[b] = 0$ in $R/\mathfrak{p}$.

Umgekehrt, sei $R/\mathfrak{p}$ ein Integritätsbereich und $ab \in \mathfrak{p}$. Dann ist $[ab] = [a][b] = 0$ in $R/\mathfrak{p}$. Daraus folgt $[a] = 0$ oder $[b] = 0$ in $R/\mathfrak{p}$. Daher, $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$.

ii) Sei $\mathfrak{m} \subseteq R$ ein Maximalideal und $\pi : R \to R/\mathfrak{m}$ die kanonische Projektion. Sei $I \subseteq R/\mathfrak{m}$ ein Ideal von $R/\mathfrak{m}$. Dann ist laut Lemma 1.1.16 $\pi^{-1}(I) \subseteq R$ ein Ideal von R. Da $[0] \in I$ und $\pi^{-1}([0]) = \mathfrak{m}$ haben wir

$$\mathfrak{m} \subseteq \pi^{-1}(I) \subseteq R.$$

Laut Definition eines Maximalideals folgt, dass $\mathfrak{m} = \pi^{-1}(I)$ oder $\pi^{-1}(I) = R$. Im ersten Fall kriegen wir $I = ([0])$, im zweiten $I = R/\mathfrak{m}$. Lemma 1.1.32 sagt nun, dass $R/\mathfrak{m}$ ein Körper sein muss.

Letztens nehmen wir an, dass $R/\mathfrak{m}$ ein Körper und $\mathfrak{m} \subsetneq I \subseteq R$ ein Ideal, welches strickt größer ist als $\mathfrak{m}$. Das heißt, es gibt ein $a \in I$, mit $a \notin \mathfrak{m}$. Daraus folgt, dass $[a] \neq 0$ in $\mathbb{R}/\mathfrak{m}$. Da $R/\mathfrak{m}$ laut Annahme ein Körper ist, gibt es ein $[b] \in R/\mathfrak{m}$ mit $[a][b] = [ab] = [1]$ in $R/\mathfrak{m}$. Daher, $[1]-[ab] = [0]$, also $1-ab \in \mathfrak{m} \subseteq I \subseteq R$. Da $a \in I$ (so war es ausgewählt), folgt, dass $ab \in I$ und daher, $(1-ab)+ab = 1 \in I$. Lemma 1.1.13 sagt nun, dass $I = R$. Als solches ist $\mathfrak{m}$ ein Maximalideal. □

Korollar 1.1.50. *Ein Maximalideal ist ein Primideal.*

Beweis. Ein Körper ist immer ein Integritätsbereich, da aus $ab = 0$, $a \neq 0$ folgt

$$b = a^{-1}ab = a^{-1}0 = 0.$$

□

Korollar 1.1.51. *Das Ring $Z/p\mathbb{Z} := Z/(p)$ ist genau dann ein Körper, wenn $p \in \mathbb{Z}$ eine Primzahl ist und wird manchmal mit $\mathbb{F}_p$ bezeichnet.*

Beweis. Dies folgt direkt aus Proposition 1.1.49 und Aufgabe 1.1.40. □

Proposition 1.1.52. *Sei K ein Körper, $R \neq \{0\}$ nicht das Nullring und $f : K \to R$ ein Ringhomomorphismus. Dann ist f immer injektiv.*

Beweis. Aufgabe 15. □

Die letzte Aussage sagt, dass man beim Ringhomomorphismus von Körpern das eine immer als Teilmenge des anderen sehen kann, was uns zum Begriff Körpererweiterung bringt:

1.2 Lokalisation

1.2.1 Lokalisation von Monoiden

Definition 1.2.1. Sei M ein Monoid und $S \subseteq M$ eine Teilmenge. Wir sage das S ein *Untermonoid* ist, wenn $1 \in S$ und für jeden $a, b \in S$ gilt $ab \in M$.

Sei M ein kommutativer Monoid und $S \subseteq M$ ein Untermonoid. Wir definieren die *lokalisation* $S^{-1}M$ von M mit S als den Quotienten von $M \times S/\sim$, wobei

$$(m_1, s_1) \sim (m_2, s_2)$$

genau dann wenn es einen Element $t \in S$ gibt mit

$$m_1 s_2 t = m_2 s_1 t.$$

Diesen t brauchen wir im Allgemeinen zum kürzen. Praktisch werden wir aber immer annehmen können, dass $t = 1$.

Öfters werden wir auch die Notation $\frac{m}{s}$ für (m, s) benutzen, da es sich ja um Brüche handelt. Es könnte aber sein, dass im Allgemeinen deutlich mehr "Brüche" gleich werden als man gewöhnt ist, sieh Lemma 1.2.23.

Lemma 1.2.2. *Die obige Relation ist eine Kongruenzrelation.*

Beweis. Aufgabe 16. □

Lemma 1.2.3. *Sei M ein Monoid und S ein Untermonoid. Die natürliche Abbildung*

$$\gamma : M \to S^{-1}M,$$

gegeben durch

$$m \mapsto (m, 1)$$

ist ein Monoidhomomorphismus.

Beweis. Aufgabe 17. □

Lemma 1.2.4. *Sei M ein Monoid und S ein Untermonoid. Es gilt*

$$\gamma(S) \subseteq (S^{-1}M)^*,$$

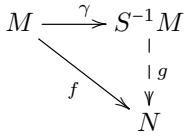
wobei $(S^{-1}M)^*$ die invertierbaren Elemente on $S^{-1}M$ bezeichnet.

Beweis. Aufgabe 17. □

Notation 1.2.5. Elemente von $S^{-1}M$ werden öfters als $\frac{a}{b}$, statt (a, b) bezeichnet.

Bemerkung 1.2.6. Die Lokalisation erfüllt eine sogenannte "universelle Eigenschaft". Eigenschaften dieser Art werden von erstaunlich vielen Sachen erfüllt und sind in der Algebra von ziemlich großer Bedeutung.

Satz 1.2.7 (Kategorische Definition)**.** *Sein M, N Monoide und $S \subseteq M$ ein Untermonoid. Sei $f : M \to N$ ein Monoidhomomorphismus, so dass $f(S) \subseteq N^*$, wo N^* die invertierbaren Elemente von N bezeichnet. Es gibt einen eindeutigen Monoidhomomorphismus $g : S^{-1}M \to N$, so dass $f = g \circ \gamma$, wo γ die kanonische Abbildung $M \to M^{-1}M$ ist. In anderen Worten, das Diagramm*



kommutiert.

Beweis. Wir definieren die Abbildung als $g\left(\frac{a}{b}\right) = f(a)f(b)^{-1}$. Dies macht Sinn, da aus $\frac{a}{b}$ direkt $b \in S$ und daher bei Annahme $f(b) \in N^*$ eine Einheit sein muss. Wir können also $f(b)^{-1}$ betrachten. Dies ist ein Monoidhomomorphismus, da $\frac{1}{1}$ auf 1 geht und

$$g\left(\frac{a}{b}\right)g\left(\frac{c}{d}\right) = f(a)f(b)^{-1}f(c)f(d)^{-1} = f(a)f(c) = f(b)^{-1}f(d)^{-1} = f(ac)f(bd)^{-1} = g\left(\frac{ac}{bd}\right).$$

Um zu sehen, dass das Diagramm kommutiert, das heißt, $g \circ \gamma = f$, sei $a \in M$. Dann gilt $(g \circ \gamma)(a) = g(\gamma(a)) = g(\frac{a}{1}) = f(a)f(1)^{-1} = f(a)$.

Als letztes wollen wir die Universalität überprüfen: Sei also $h : S^{-1}M \to N$ ein Abbildung, so dass das Diagramm kommutiert. In anderen Worten, $h\left(\frac{a}{1}\right) = h(\gamma(a)) = f(a)$, für jeden $a \in M$. Sei nun $\frac{a}{b} \in S^{-1}M$ beliebig. Dann gilt

$$h\left(\frac{a}{b}\right)h\left(\frac{b}{1}\right) = h\left(\frac{a}{1}\right) = f(a)$$

auf einer Seite und

$$h\left(\frac{a}{b}\right)h\left(\frac{b}{1}\right) = h\left(\frac{a}{b}\right)f(b)$$

auf der Anderen. Da aber $f(b) \in N^*$ bei Annahme gelten muss, können wir diese zwei Gleichungen zusammenfassen und als

$$h\left(\frac{a}{b}\right) = f(a)f(b)^{-1} = g\left(\frac{a}{b}\right)$$

umformen. Dies beweist die Aussage. □

Korollar 1.2.8. *Sei M ein Monoid und G eine abelsche Gruppe. Für jeden Monoidhomomorphismus $f : M \to G$ gibt es ein eindeutiges Monoidhomomorphismus $g : M^{-1}M \to G$, so dass $f = g \circ \gamma$.*

Definition 1.2.9. Ein Monoid M heißt *kürzbar*, wenn für alle $a, b, c \in M$, $ab = ac \Rightarrow b = c$.

Proposition 1.2.10. *Sei M ein kommutativer Monoid. Die Lokalisation $M^{-1}M$ ist eine abelsche Gruppe und die natürliche Abbildung*

$$M \to M^{-1}M, \quad m \mapsto (m, 1)$$

ist genau dann injektiv, wenn M kürzbar ist.

Beweis. Aufgabe 17. □

Die zu M assoziierte abelsche Gruppe $M^{-1}M$ wird als die *Grothendieck Gruppe* bezeichnet und öfters mit M^{Gr} notiert.

Die Proposition gilt etwas allgemeiner. Wenn $S \subseteq M$ ein Untermonoid ist, so dass aus $ac = bc, c \in S$ folgt $a = b$, dann ist die kanonische Abbildung $M \to S^{-1}M$ immer injektiv.

Beispiel 1.2.11.
- Sei $M = \mathbb{N}$ das Monoid der natürlichen Zahlen unter Addition. Dann ist $\mathbb{N}^{-1}\mathbb{N} \simeq \mathbb{Z}$, die abelsche Gruppe der ganzen Zahlen.

- Sei G eine abelsche Gruppe. Dann ist $S^{-1}G \simeq G$ für jeden Untermonoiden $S \subseteq G$.

Das zweite Beispiel gilt allgemeiner:

Lemma 1.2.12. *Sei M ein kommutatives Monoid und $G \subseteq M$ eine Untergruppe. Es gilt $G^{-1}M \simeq M$.*

Beweis. Vom Satz 1.2.7 folgt direkt (indem man $f = \mathsf{Id} : M \to M$ nimmt), dass es ein $g : G^{-1}M \to M$ gibt, so dass $g \circ \gamma = \mathsf{Id}$. Von der Konstruktion des selbes Satzes haben wir auch, dass dies durch $\frac{a}{b} = ba^{-1}$ gegeben wird.

Es bleibt nur noch zu zeigen, dass $\gamma \circ g : G^{-1}M \to G^{-1}M$ die Identität ist. Doch dies ist klar, denn es gilt $(\gamma \circ g)\left(\frac{a}{b}\right) = \gamma(ab^{-1}) = \frac{ab^{-1}}{1} \sim \frac{a}{b}$, da $ab^{-1}b = a$. □

1.2.2 Lokalisation von Ringen

Sei R ein Ring. Dann kann R auch als ein kommutatives Monoid aufgefasst werden, indem wir die Addition vergessen. Daher können wir auch ein Ring lokalisieren.

Proposition 1.2.13. *Sei R ein Ring und $S \subseteq R$ ein multiplikatives Untermonoid. Dann hat $S^{-1}R$ eine natürliche Ringstruktur, wobei*

$$(m_1, s_1) + (m_2, s_2) := (m_1 s_2 + m_2 s_1, s_1 s_2).$$

Beweis. Aufgabe 16. □

Satz 1.2.14 (Kategorische Definition)**.** *Sein R, T Ringe, $S \subseteq R$ ein multiplikatives Untermonoid und $f : R \to T$ ein Ringhomomorphismus, so dass $f(S) \subseteq T^*$, wo T^* die invertierbaren Elemente von T sind. Dann gibt es ein eindeutiges Ringhomomorphismus $g : S^{-1}R \to T$, so dass $f = g \circ \gamma$, wo $\gamma : R \to S^{-1}R$ die kanonische Abbildung ist.*

Beweis. Nach Satz 1.2.7 ist das einzige, das wir noch zu beweisen haben, dass die Abbildung g, welches durch $g\left(\frac{a}{b}\right) = f(a)f(b)^{-1}$ gegeben ist, mit der Addition verträglich ist. Es gilt

$$\begin{aligned} g\left(\frac{a}{b} + \frac{c}{d}\right) &= g\left(\frac{ad + bc}{bd}\right) \\ &= f(ad + bc)f(bd)^{-1} \\ &= f(a)f(d)f(b)^{-1}f(d)^{-1} + f(b)f(c)f(b)^{-1}f(d)^{-1} \\ &= f(a)f(b)^{-1} + f(c)f(d)^{-1} \\ &= g\left(\frac{a}{b}\right) + g\left(\frac{c}{d}\right). \end{aligned}$$

□

Notation 1.2.15. Sei R ein Integritätsbereich. Dann ist $S = R \setminus 0$ ein Untermonoid von R und wir können damit Lokalisieren. In diesem speziellen Fall werden wir die Notation $Q(R) := (R \setminus \{0\})^{-1}R$ benutzen.

Proposition 1.2.16. *Sei R ein Integritätsbereich. Dann ist $Q(R)$ ein Körper und die natürliche Abbildung $\gamma : R \to Q(R)$ ist injektiv.*

Beweis. Sei $0 \neq \frac{a}{b} \in Q(R)$. Da $a = 0$ impliziert $\frac{a}{b} = \frac{0}{b} \sim \frac{0}{1}$ ($01 = 0b$), muss $\frac{b}{a} \in Q(R)$. Als solches ist $\frac{a}{b}$ invertierbar, denn es gilt $\frac{a}{b}\frac{b}{a} \sim \frac{1}{1} = 1$.

Injektivität Aufgabe 17, nachdem man $ac = bc$ zu $ac - bc = (a - b)c$ umformt. Als solches ist die Implikation $ac = bc \Rightarrow a = b$ äquivalent zur Integritätseigenschaft. □

Als solches wird $Q(R)$ als das *Quotientenkörper* von R bezeichnet.

Bemerkung 1.2.17. Als Zusammenfassung: Es gibt 2 Möglichkeiten einen Körper von einem Integritätsbereich zu erstellen:

- R durch einen Maximalideal $\mathfrak{m}$ teilen;
- Alles außer 0 invertieren.

Bemerkung 1.2.18. Das direkte Analog zu Korollar 1.2.8 hält nicht für Ringe: ein Ringhomomorphismus in einem Körper muss nicht durch den assoziierten Körper faktorisieren. Der Grund dafür ist die Tatsache, dass wir in einem Ring/Körper zusätzlich die Null haben. Z.B. haben wir die Abbildung $\mathbb{Z} \to \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $n \mapsto n \bmod p$. Es gibt aber kein Ringhomomorphismus von $\mathbb{Q}$ nach $\mathbb{F}_p$.

Korollar 1.2.19. *Sei R ein Integritätsbereich, K ein Körper und $f : R \to K$ ein injektives Ringhomomorphismus. Dann gibt es ein eindeutiges Ringhomomorphismus $g : Q(R) \to K$, so dass $f = g \circ \gamma$, wo γ wie oben ist.*

Beweis. Von Satz 1.2.14 wissen wir, dass es einen eindeutigen Ringhomomorphismus $g : Q(R) \to K$ gibt, wenn $f(R \setminus \{0\}) \subseteq K^*$. Da aber $K^* = K \setminus \{0\}$, ist dies Äquivalent zu sagen, dass $\mathsf{Ker}(f) = \{0\}$, was Injektivität bedeutet. □

Korollar 1.2.20. *Sei R ein Ring. Es gibt höchstens ein Ringhomomorphismus $\mathbb{Q} \to R$.*

Beweis. Aufgabe 18. □

Lemma 1.2.21. *Sei R ein Ring und $G \subseteq R$ eine multiplikative Untergruppe. Dann gilt $G^{-1}R \simeq R$.*

Beweis. Den Hauptteil haben wir schon in Lemma 1.2.12 beweisen. Es bleibt zu zeigen, dass die dort definierte Abbildung γ^{-1} auch mit der Addition Verträglich ist. Dies braucht man eigentlich nicht zeigen, da das inverse immer alle algebraischen Strukturen erhält. Da wir diese allgemeine Aussage aber nicht benutzen wollen, argumentieren wir wie folgt:

$$\gamma^{-1}\left(\frac{r}{g}\right) + \gamma^{-1}\left(\frac{r'}{g'}\right) = rg^{-1} + r'(g')^{-1}$$

und

$$\gamma^{-1}\left(\frac{rg' + r'g}{gg'}\right) = (rg' + r'g)\,(gg')^{-1} = (rg' + r'g)(g')^{-1}g^{-1} = rg^{-1} + r'(g')^{-1}.$$

□

Bemerkung 1.2.22. (Fast) ausnahmslos wird bei Ringen verlangt, dass $S \subseteq R$ <u>nicht</u> die Null enthält. Der Grund dafür ist die folgende Aussage:

Lemma 1.2.23. *Sei R ein Ring und $S \subseteq R$ ein Untermonoid mit $0 \in S$. Dann gilt*

$$S^{-1}R \simeq 0,$$

wobei 0 den Nullring bezeichnet.

Beweis. Aufgabe 19. □

Aufgaben 2

Aufgabe 9 (1 Punkt). Beweise, dass ein Ring R genau dann ein Integritätsbereich ist, wenn $\{0\} = (0) \subseteq R$ ein Primideal ist.

Aufgabe 10 (2 Punkte). Sei $I \subseteq R$ ein Ideal eines Ringes R. Zeige, dass R/I wirklich ein Ring ist. Das heißt, dass Assoziativität, Distributivität, Wohldefiniertheit etc. erfüllt sind.

Aufgabe 11 (1 Punkt). Sei $f : R \to S$ ein Ringhomomorphismus. Zeige, dass das Kern $\mathsf{Ker}(f) \subseteq R$ ein Ideal von R ist.

Aufgabe 12 (2 Punkt). Sein A, B abelsche Gruppen und $f : A \to B$ ein Gruppenhomomorphismus. Der sogenannte *erste Isomorphiesatz* besagt, dass die Abbildung

$$A/\mathsf{Ker}(f) \to \mathsf{Bild}(f),$$

gegeben durch $[a] \mapsto f(a)$, ein (wohldefinierter) Gruppenisomorphismus ist. Sein, des weiteren, A und B mit Ringstrukturen versehen und sei $f : A \to B$ zusätzlich ein Ringhomomorphismus. Unter Annahme des ersten Isomorphiesatzes für Gruppen, zeige, dass der kanonische Isomorphismsus

$$R/\mathsf{Ker}(f) \simeq \mathsf{Bild}(f)$$

ein Ringhomomorphismus ist.

In anderen Worten, beweise den ersten Isomorphiesatz für Ringe, wenn man es für Gruppen schon kennt.

Aufgabe 13 (2 Punkt). Sei R ein Ring und $I \subseteq J \subseteq R$ Ideale von R. Zeige, dass

$$R/J = (R/I)/(J/I).$$

Aufgabe 14 (1 Punkt). Zeige, dass ein Ringhomomorphismus $f : R \to S$ genau dann injektiv ist, wenn der Kern $\mathsf{Ker}(f) = (0) = \{0\}$ trivial ist.

Aufgabe 15 (1 Punkt). Sei K ein Körper und $R \neq \{0\}$ nicht das Nullring. Beweise, dass ein Ringhomomorphismus $f : K \to R$ immer injektiv ist.

Aufgabe 16 (2 Punkte insgesamt). Sei M ein Monoid und $S \subseteq M$ ein Untermonoid.

1. (1 Teilpunkt) Beweise, dass $S^{-1}M$, definiert wie in der Vorlesung, ein Monoid ist. Das heißt, zeig, dass die Relation $\simeq$ auf $S^{-1}M$, gegeben durch

   $$(m_1, s_1) \simeq (m_2, s_2),$$

   genau dann wenn es einen Elementen $t \in S$ gibt mit

   $$m_1 s_2 t = m_2 s_1 t,$$

   eine Kongruenzrelation ist.

2. (1 Teilpunkt) Habe $M = R$ nun eine zusätzliche Ringstruktur. Beweise, dass unter

   $$(m_1, s_1) + (m_2, s_2) := (m_1 s_2 + m_2 s_1, s_1 s_2),$$

   $S^{-1}R$ ein Ring wird. Also, dass die obige Kongruenzrelation mit dieser Addition verträglich ist.

Aufgabe 17 (4 Punkte insgesamt). 1. (1 Teilpunkt) Sei M ein kommutativer Monoid, $S \subseteq M$ ein Untermonoid und $S^{-1}M$ die Lokalisation von M mit S. Zeige, dass die Zuordnung

$$\gamma : M \to S^{-1}M, \quad m \mapsto (m, 1),$$

ein Monoidhomomorphismus ist. Wenn $M = R$ ein Ring ist, beweise, dass dies auch ein Ringhomomorphismus ist.

2. (1 Teilpunkt) Beweise, dass unter $\gamma : M \to S^{-1}M$, $S \subseteq M$ in die Einheiten von $S^{-1}M$ geht. Also, dass $\gamma(S) \subseteq (S^{-1}M)^*$.

3. (1 Teilpunkt) Zeige, dass γ genau dann injektiv ist (auf ganz M), wenn $ac = bc$ impliziert $a = b$ für jeden $a, b \in M$ und $c \in S$. Schlussfolgere, dass die Lokalisation $M^{-1}M$ eine abelsche Gruppe und die natürliche Abbildung

$$M \to M^{-1}M, \quad m \mapsto (m, 1)$$

genau dann injektiv ist, wenn aus $ac = bc$, folgt, dass $a = b$ für jeden $a, b, c \in M$.

4. (1 Teilpunkt) Sei R ein Integritätsbereich. Beweise mithilfe des obigen Arguments, dass $(R \setminus \{0\})^{-1}R$ ein Körper ist und dass die natürliche Abbildung $R \to (R \setminus \{0\})^{-1}R$ injektiv ist.

Aufgabe 18 (1 Punkt). Sei R ein Ring. Beweise, dass es höchstens ein Ringhomomorphismus $\mathbb{Q} \to R$ gibt.

Aufgabe 19 (1 Punkt). Sei R ein Ring und $S \subseteq R$ ein Untermonoid mit $0 \in S$. Beweise, dass $S^{-1}R \simeq \{0\}$ das Nullring ist.

1.3 Körpererweiterungen

1.3.1 Algebraische Elemente

Definition 1.3.1. Sei $\varphi : K \to L$ ein Ringhomomorphism und K, L Körper. Dann wird K ein *Unterkörper* bzw. *Teilkörper* von L genannt und L eine *Körpererweiterung* von K. Die Abbildung φ wird öfters *Einbettung* genannt.

Bemerkung 1.3.2. Der Begriff Unterkörper mag, rein von der Definition, etwas verwirrend klingen. Aber wie schon angesprochen, rechtfertigt Proposition 1.1.52 den Begriff. Für jede Abbildung $\varphi : K \to L$ gilt bekanntlich $\mathsf{Bild}(\varphi) \subseteq L$. Aus Injektivität (was aus der Tatsache, dass K ein Körper ist) folgt aber, dass $\mathsf{Bild}(\varphi) \simeq K$ eine Isomorphie ist. Daher können wir K, bis auf Isomorphie, als eine Teilmenge von L auffassen.

In unseren Hauptfällen, welche Körpererweiterungen von $\mathbb{Q}$ sein werden, ist es jedoch noch klarer. Da $\mathbb{Z}$ unter den Ringen initial ist (es gibt genau einen Ringhomomorphismus $f : \mathbb{Z} \to R$), gibt es maximal einen Ringhomomorphismus von $\mathbb{Q}$ nach einem beliebigen Körper K (Korollar 1.2.20). Es folgt, dass es genau eine Einbettung $\varphi : \mathbb{Q} \to L$ für irgendeinen Körper L gibt. Als solches kann man $\mathbb{Q}$ *kanonisch* als eine Teilmenge von L auffassen, wenn L eine Körpererweiterung von $\mathbb{Q}$ ist.

Definition 1.3.3. Sei L eine Körpererweiterung von K. Ein Element $\alpha \in L$ heißt *Algebraisch über* K, wenn es ein Polynom $0 \neq f \in K[X]$ gibt, so dass $f(\alpha) = 0$.

Mit $f(\alpha)$ meinen mir, um technisch genau zu sein, $\varphi(f)(\alpha)$. Das heißt, ein Polynom

$$f(x) := a_0 + a_1 x + \ldots + a_n x^n$$

wird zu

$$\varphi(f)(x) := \varphi(a_0) + \varphi(a_1)x + \ldots + \varphi(a_n)x^n$$

hochgehoben und dann α eingesetzt. Praktisch werden wir uns darum nicht weiter kümmern brauchen, da es in unseren Hauptfällen nur einen einzigen φ geben wird, sieh unsere Diskussion im zweiten Abschnitt der Bemerkung 1.3.2.

Zu einem algebraischen Element α über K können wir folgende Objekte zuordnen:
Ein Ring

$$K[\alpha] := \{f(\alpha) \mid f \in K[X]\},$$

ein Körper

$$K(\alpha) := \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f, g \in K[X], g(\alpha) \neq 0 \right\}$$

und ein Ideal

$$I(\alpha) := \{f \in K[X] \mid f(\alpha) = 0\}.$$

Lemma 1.3.4. *Für jedes algebraische Element α ist $K[\alpha]$ ein Ring, $K(\alpha)$ ein Körper und $I(\alpha)$ ein Ideal.*

Beweis. Alle Eigenschaften sind elementar zum Überprüfen, z.B., wenn $f(\alpha), g(\alpha) \in K[\alpha]$ dann gilt $g(\alpha) + f(\alpha) = (g + f)(\alpha) \in K[\alpha]$. □

All diese Objekte stark zueinander verbunden sind. Natürlich haben wir

$$K \subseteq K[\alpha] \subseteq K(\alpha) \subseteq L.$$

Doch es stimmt noch mehr, wie wir es bald zeigen werden.

1.3.2 Normierte Polynome

Definition 1.3.5. Ein Polynom heißt *normiert*, (bzw. *monisch*), wenn der Leitkoeffizient 1 ist.

Beispiel 1.3.6. Das Polynom $x^2 + 5$ ist normiert. Das Polynom $2x^2 + 5$ ist *nicht* normiert, jedoch ist $x^2 + \frac{5}{2}$ normiert.

Lemma 1.3.7. *Für jeden Körper K und jedes Ideal $(0) \neq I \subseteq K[X]$ gibt es genau ein normiertes Polynom $\mathfrak{m} \in K[X]$ über K, so dass*

$$I = (\mathfrak{m}).$$

Beweis. Man erinnere sich zuerst, dass $K[X]$ ein Hauptidealbereich ist (Proposition 1.1.26). Es gibt daher ein Polynom $0 \neq \mathfrak{m}' \in K[X]$, so dass $(\mathfrak{m}') = I$. Sei a_n das Leitkoeffizient von $\mathfrak{m}'$ und definiere $\mathfrak{m} := \mathfrak{m}'/a_n$. (In anderen Worten, normalisiere). Dann ist $\mathfrak{m}$ ein normiertes Polynom und $(\mathfrak{m}') = (\mathfrak{m})$ laut Korollar 1.1.20, da $0 \neq a_n \in K^\times$ und daher eine Einheit in $K[X]$ ist.

Um die Eindeutigkeit von $\mathfrak{m}$ zu sehen, sei $\mathfrak{n}$ ein weiteres normiertes Polynom, so dass $(\mathfrak{n}) = (\mathfrak{m})$. Daher, $(\mathfrak{n}) \subseteq (\mathfrak{m})$ und $(\mathfrak{m}) \subseteq (\mathfrak{n})$. Laut Lemma 1.1.19 ist dies äquivalent zu sagen, dass $\mathfrak{n}|\mathfrak{m}$ und $\mathfrak{m}|\mathfrak{n}$. Es folgt von Lemma 1.1.9, dass $\mathsf{grad}(\mathfrak{n}) = \mathsf{grad}(\mathfrak{m})$ und daher $\mathfrak{n} = f\mathfrak{m}$ mit $\mathsf{grad}(f) = 0 \Rightarrow f(x) = a$ mit $a \in K$ (Lemma 1.1.9). Da sowohl $\mathfrak{m}$ wie auch $\mathfrak{n}$ normiert sind, muss $a = 1$ und daher $\mathfrak{n} = \mathfrak{m}$ sein. □

Korollar 1.3.8 (Definition)**.** *Sei K ein Körper und α ein algebraisches Element über K. Es gibt genau ein normiertes Polynom $\mathfrak{m}_\alpha$ über K, so dass*

$$I(\alpha) = (\mathfrak{m}_\alpha).$$

Dieses $\mathfrak{m}_\alpha$ wird das Minimalpolynom *von α genannt.*

1.3.3 Irreduzible, reduzible und invertierbare Elemente

Definition 1.3.9. Sei R ein kommutatives Ring. Wir können die Elemente von R, ungleich Null, in die folgenden drei Kategorien einteilen:

- Ein Element $x \in R$ heißt *invertierbar* (bzw. eine Einheit), wenn es ein Element $y \in R$ gibt, mit $xy = 1$.
- Ein Element $x \in R$ heißt *irreduzibel*, wenn x nicht invertierbar ist, $x \neq 0$ und aus $x = yz$ folgt, dass y oder z invertierbar in R ist.
- Ein Element (ungleich Null) heißt *reduzibel*, (oder *zerlegbar*) wenn es weder invertierbar noch irreduzibel ist.

Für einen Polynomring über einem Körper können wir das ganze etwas vereinfachen. Sei $K^\times := K \setminus \{0\}$ die Einheiten von K. Dann gilt

Lemma 1.3.10.
- *Ein Element $f(x) \in K[X]$ ist genau dann invertierbar wenn $f(x) \in K^\times$, wobei $K^\times = K \setminus \{0\}$ die Einheiten von K sind. In anderen Worten, wenn $\mathsf{grad}(f) = 0$.*
- *Ein Element $f(x) \in K[X]$ ist irreduzibel, genau dann wenn $\mathsf{grad}(f) \geq 1$ und aus $f(x) = g(x)h(x)$ folgt $\mathsf{grad}(g) = 0$ oder $\mathsf{grad}(h) = 0$.*

Beispiel 1.3.11. Die folgenden Polynome sind irreduzibel:

(i) Die konstante Funktion $f(x) = p \in \mathbb{Z}[X]$, für $p \in \mathbb{Z}$ Primzahl.

(ii) $f(x) = x - a \in R[X]$ für jeden Integritätsbereich R und jedes $a \in R$.

(iii) $f(x) = x^2 - 2 \in \mathbb{Q}[X]$

(iv) $f(x) = x^2 + 2 \in \mathbb{R}[X]$.

Die folgenden Polynome sind reduzibel:

(i) Die konstante Funktion $f(x) = p \in \mathbb{Q}[X]$, für jeden $p \in \mathbb{Q}$.

(ii) $f(x) = x^2 - 2 \in \mathbb{R}[X]$

(iii) $f(x) = x^2 + 2 \in \mathbb{C}[X]$

(iv) $f(x) = x^2 - 1 \in \mathbb{Z}[X]$.

Irreduzible Polynome sind mit Maximalidealen eng verbunden:

Proposition 1.3.12. *Sei K ein Körper. Die Maximalideale von $K[X]$ sind genau von der Form $(\mathfrak{m})$, wobei $\mathfrak{m}$ ein irreduzibles Polynom über K ist.*

Beweis. Wie schon in Proposition 1.1.26 bewiesen ist $I = (\mathfrak{m})$ für irgendein $\mathfrak{m} \in K[X]$. Sei I ein Maximalideal. Als erstes ist $\mathfrak{m} \neq 0$, da $(0) \subsetneq (x)$, für einen beliebigen $0 \neq x \in K[X]$. Als zweites bemerken wir, dass $\mathsf{grad}(\mathfrak{m}) \geq 1$, denn aus $\mathsf{grad}(\mathfrak{m}) = 0$ folgt (Lemma 1.3.10), dass $\mathfrak{m}$ invertierbar ist und daher wäre $(\mathfrak{m}) = 1$. Sei $\mathfrak{m} = fg$. Lemma 1.1.19 besagt nun, dass $(\mathfrak{m}) \subseteq (f) \subseteq K[X]$. Da I maximal war, muss $(\mathfrak{m}) = (f)$ oder $(f) = K[X]$ gelten. Die erste Gleichung impliziert $(f) \subseteq (\mathfrak{m}) \Leftrightarrow \mathfrak{m}|f \Rightarrow \mathsf{grad}(\mathfrak{m}) = \mathsf{grad}(f)$. Daher ist $\mathsf{grad}(g) = 0$ (1. von Prop. 1.1.9). Aus $(f) = K[X]$ folgt $\mathsf{grad}(f) = 0$. Somit ist $\mathfrak{m}$ irreduzibel, laut Lemma 1.3.10.

Auf der andere Seite, sei $\mathfrak{m}$ irreduzibel und $(\mathfrak{m}) \subseteq I = (f) \subseteq K[X]$ sei gegeben. Lemma 1.1.19 impliziert, dass $\mathfrak{m} = fg, g \in K[X]$. Irreduzibilität von $\mathfrak{m}$ impliziert, mithilfe von Lemma 1.3.10, dass $\mathsf{grad}(\mathfrak{m}) \geq 1$ (also $(\mathfrak{m}) \neq (1)$ und $\mathsf{grad}(f) = 0$ oder $\mathsf{grad}(g) = 0$. Aus $\mathsf{grad}(f) = 0$ folgt $(f) = K[X]$ und aus $\mathsf{grad}(g) = 0$ folgt $(f) = (\mathfrak{m})$. Also ist $(\mathfrak{m})$ maximal. □

Proposition 1.3.13. *Für jedes algebraische Element α gilt $I(\alpha) = (\mathfrak{m}_\alpha)$ ein Maximalideal. Äquivalent, das Minimalpolynom $\mathfrak{m}_\alpha$ ist ein irreduzibles Polynom.*

Beweis. Sei $\mathfrak{m}_\alpha = fg$. Dann gilt

$$\mathfrak{m}_\alpha(\alpha) = f(\alpha)g(\alpha) = 0.$$

Da $K[X]$ ein Integritätsbereich ist, gilt o.B.d.A $f(\alpha) = 0$. Da $(\mathfrak{m}_\alpha) = I(\alpha) = \{f \in K[X] \mid f(\alpha) = 0\}$ (Korollar 1.3.8), folgt $f(x) \in (\mathfrak{m}_\alpha)$ und daher $\mathfrak{m}_\alpha|f$. Bei Annahme ist auch $f|\mathfrak{m}_\alpha$ und daher gilt $\mathsf{grad}(\mathfrak{m}_\alpha) = \mathsf{grad}(f)$ (Lemma 1.1.9). Dies impliziert $\mathsf{grad}(g) = 0$ und so ist $\mathfrak{m}_\alpha$ irreduzibel. Proposition 1.3.12 oben besagt, dass $(\mathfrak{m}_\alpha)$ maximal ist. □

Proposition 1.3.14. *Ein Polynom $\mathfrak{m}$ ist genau dann das Minimalpolynom eines algebraischen Elements α, wenn es die folgenden drei Eigenschaften erfüllt:*

- $\mathfrak{m}(\alpha) = 0$,
- $\mathfrak{m}$ *normiert ist und*
- $\mathfrak{m}$ *irreduzibel ist.*

Beweis. Eine Seite wurde in Proposition 1.3.13 bewiesen. Für die andere Seite, sei $\mathfrak{m}$ normiert, irreduzibel und $\mathfrak{m}(\alpha) = 0$. Dann ist $\mathfrak{m} \in I(\alpha)$ bei Definition. Da $I(\alpha) = (\mathfrak{m}_\alpha)$ ist $\mathfrak{m} \in (\mathfrak{m}_\alpha)$. Also, $\mathfrak{m} = f\mathfrak{m}_\alpha$ für irgendein $f \in K[X]$. Die Irreduzibilität von $\mathfrak{m}$ sagt nun, dass $f(x)$ invertierbar ist. Korollar 1.1.20 beendet den Beweis. □

Satz 1.3.15. *Sei K ein Körper und α algebraisch über K. Dann gibt es Isomorphien von Ringen*

$$K[X]/I(\alpha) \xrightarrow{\Phi} K[\alpha] \xrightarrow{\Gamma} K(\alpha).$$

Beweis. Zur Erinnerung, $I(\alpha) = (\mathfrak{m}_\alpha)$.

Φ: Wir definieren die Abbildung $\Phi(\overline{f}) = f(\alpha)$, wobei $\overline{f}$ für $f + (\mathfrak{m}_\alpha)$ steht.

Als erstes zeigen wir, dass die Abbildung wohldefiniert ist. Sei $\overline{f} = \overline{g}$. Dann ist $\overline{f} - \overline{g} = \overline{f - g} = \overline{0}$, also $f - g \in (\mathfrak{m}_\alpha)$. Daher, $(f - g)(\alpha) = 0 \Leftrightarrow f(\alpha) - g(\alpha) = 0$ und somit gilt $f(\alpha) = g(\alpha)$.

Als nächstes zeigen wir, dass es ein Ringhomomorphismus ist.

- $\Phi(\overline{1}) = 1$ ist klar.
- $\Phi(\overline{f + g}) = (f + g)(\alpha) = f(\alpha) + g(\alpha) = \Phi(\overline{f}) + \Phi(\overline{g})$
- $\Phi(\overline{fg}) = (fg)(\alpha) = f(\alpha)g(\alpha) = \Phi(\overline{f})\Phi(\overline{g})$

Es ist klar, dass Φ surjektiv ist, da für jeden $f(\alpha)$, $\Phi(\overline{f}) = f(\alpha)$.

Um zu zeigen, dass Φ injektiv ist benutzen wir Proposition 1.3.13 um zu sehen, dass $(\mathfrak{m}_\alpha)$ ein Maximalideal ist. Daher ist $K[X]/(\mathfrak{m}_\alpha)$ ein Körper laut Proposition 1.1.49. Das Resultat folgt nun von Proposition 1.1.52.

Γ: Es ist direkt Ersichtlich, dass $K(\alpha)$ der Quotientenkörper von $K[\alpha]$ ist. Also, dass $K(\alpha) = Q(K[\alpha]) = (K[\alpha] \setminus 0)^{-1}K[\alpha]$ gilt. Die Abbildung Γ ist die kanonische Abbildung $f(\alpha) \mapsto \frac{f(\alpha)}{1}$, wobei 1 als das konstante Polynom aufgefasst wird. Wir könnten auch $1(\alpha)$ schreiben. Laut Lemma 1.2.21 reicht es aus zu zeigen, dass jedes Element $0 \neq f(\alpha) \in K[\alpha]$ invertierbar ist. Dies folgt direkt aus der Tatsache, das $K[\alpha]$ ein Körper ist, wie im vorigen Teil bewiesen.

□

1.3.4 Grad einer Körpererweiterung

Module Da wir Module nicht für den weiten Kurs brauchen, werden wir die folgenden drei Aussagen nicht beweisen. Die Beweise sind aber recht einfach und können per Hand überprüft werden.

Definition 1.3.16. Sei R ein Ring und M eine abelsche Gruppe. Dann heißt M, zusammen mit einer Abbildung $\cdot : R \times M \to M$, (wobei wir dir Notation rm statt $\cdot(r, m)$ benutzen), ein *Modul* über R, oder einfach R-Modul, wenn für alle $m, n \in M$, $r, s \in R$

- $1m = m$, $1 \in R$;
- $r(m + n) = rm + rn$;
- $(r + s)m = rm + sm$;
- $(rs)m = r(sm)$

gilt.

Es folgt von den Axiomen, dass $r0 = 0$ erfüllt ist. Wir werden einfach M sagen, nicht $(M, \cdot)$, obwohl die Abbildung natürlich teil der Struktur ist. Es ist nicht schwer zu sehen, dass dies Äquivalent zu der folgenden Definition ist:

Proposition 1.3.17 (Definition)**.** *Sei M eine abelsche Gruppe und $\mathsf{End}(M)$ das (nicht-kommutative) Ring der Endomorphismen. Eine Abbildung $f : R \to \mathsf{End}(M)$ definiert ein Modul, genau dann wenn f ein Ringhomomorphismus ist. Mehr als das, die R-Modulstrukturen von M sind in eine 1-1 Beziehung zu den gegebenen Ringhomomorphismen.*

Beweis. Aufgabe. Die Idee ist, bei der Abbildung $\cdot : R \times M \to M$, ein Element $r \in R$ zu fixieren, und es als $f_r : M \to M$, $m \mapsto rm$ zu sehen. Dies ist klar ein Endomorphismus von M. Dann ist f die Abbildung, die durch $r \mapsto f_r$ definiert ist. □

Definition 1.3.18. Sein M, N zwei R-Module. Ein Gruppenhomomorphismus $f : M \to N$ ist ein *R-Modulhomomorphismus* wenn für alle $m \in M$ und $r \in R$ gilt

$$f(rm) = rf(m).$$

Alternativ: Eine Abbildung $f : M \to N$ ist ein R-Modulhomomorphismus, wenn für alle $m, n \in M$, $r, s \in R$ gilt:

$$f(rm + sn) = rf(m) + sf(n).$$

Proposition 1.3.19. *$\mathbb{Z}$-Module sind genau abelsche Gruppen und $\mathbb{Z}$-Modulhomomorphismen sind genau Gruppenhomomorphismen.*

Beweis. Aufgabe. □

Definition 1.3.20. Ein *Vektorraum* ist ein Modul über einen Körper. *Vektorraum Homomorphismen* sind genau Modulhomomorphismen.

Lemma 1.3.21. *Sein R, S Ringe und $f : R \to S$ ein Ringhomomorphismus. Dann ist S ein R-Modul in natürlicher weise: Wir vergessen die Multiplikation in S und fassen es als eine abelsche Gruppe auf und definieren*

$$rs := f(r)s.$$

Beweis. Aufgabe. □

Besonders wichtig für diesen Kurs ist der Fall, wenn R, S Körper sind. In diesem Fall können wir (leichter) von Dimension, bzw. Grad reden. Dazu, kurz zur Erinnerung, was Basis und Dimension von Vektorräumen sind.

Definition 1.3.22. Sei V ein Vektorraum über einem Körper K. Eine Teilmenge $B = \{e_1, \ldots\} \subseteq V$ heißt *Basis* wenn folgendes gilt:

- Wir können jedes Element $v \in V$ als Linearkombination von B schreiben: Also als

  $$v = r_1 e_1 + \cdots + r_i e_i + \cdots$$

  wobei $r_i \in R$ und *fast alle* Null sind. Fast alle bedeutet, dass es nur endlich viele r_i's gibt, welche ungleich Null sind. Dies wird (*erzeugendes System*) genannt.

- Die Elemente von B sind linear Unabhängig: Also aus

  $$0 = r_1 e_1 + \cdots + r_i e_i + \cdots$$

  folgt, dass alle Koeffizienten r_i-s null sind (*lineare Unabhängigkeit*).

Definition 1.3.23. Sei V ein K-Vektorraum. Die *Dimension* von V über K, geschrieben $\dim_K(V)$, ist die Anzahl der Elemente einer Basis B von V, wenn B endlich ist. In anderen Worten

$$\dim_K(V) := \#|B|.$$

In diesem Fall heißt B *endlich dimensional*. Wenn B unendlich ist, dann sagen wir $\dim_K(V) = \infty$.

Es ist nicht so einfach von der Dimension eines Moduls im Allgemeinen zu reden. Aber wir können immer von *endlich erzeugt* sprechen. Ein R-Modul M ist endlich erzeugt wenn es ein endliches erzeugendes System hat.

Beispiel 1.3.24.

- Endlich erzeugte $\mathbb{Z}$-Modulen sind genau endlich erzeugte abelschen Gruppen.
- Ein Beispiel eines *nicht* endlich erzeugten $\mathbb{Z}$-Moduls ist $\mathbb{Q}$.
- Ein Beispiel von *nicht* endlich erzeugten $\mathbb{Q}$-Vektorräumen ist $\mathbb{R}$.

Definition 1.3.25. Seien K, L Körper und $f : K \to L$ eine Körpererweiterung. Dann nennen wir $[L : K]$ den Grad der Erweiterung und definieren es als die Dimension von L als K-Vektorraum: In anderen Worten

$$[L : K] \coloneqq \dim_K(L).$$

Beispiel 1.3.26.

- $[\mathbb{C} : \mathbb{R}] = 2$;
- $[\mathbb{Q}[\sqrt{2}], \mathbb{Q}] = 2$;
- $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$.

Lemma 1.3.27. *Sei $f \in K[X]$ ein irreduzibles Polynom vom Grad d. Dann ist $\{1, X, X^2, \ldots, X^{d-1}\}$ eine Basis von $K[X]/(f)$. In anderen Worten, es gilt*

$$[K[X]/(f) : K] = d.$$

Beweis. Aufgabe 20. □

Lemma 1.3.28. *Sei α ein algebraisches Element über K. Dann ist $[K(\alpha) : K] = \mathsf{grad}(\mathfrak{m}_\alpha)$.*

Beweis. Aufgabe + voriges Beispiel 1.3.27. □

Lemma 1.3.29. *Ein Element $\alpha \in \mathbb{C}$ ist genau dann algebraisch über K, wenn $[K(\alpha) : K] < \infty$.*

Beweis. Eine Seite ist Lemma 1.3.28, denn wenn α algebraisch über K ist, dann hat es einen Minimalpolynom und dieser ist freilich vom endlichen Grad.

Auf der anderen Seite, wenn der Grad der Erweiterung $[K(\alpha) : K]$ endlich ist können die Elemente $\{1, \alpha, \alpha^2, \ldots, \alpha^d, \cdots\}$ *nicht* linear unabhängig sein. Daher gibt es $\{a_i\} \in K$, so dass $\sum a_i \alpha^i = 0$. In anderen Worten gibt es ein Polynom, $f(x) = \sum a_i x^i$, mit $f(\alpha) = 0$. Daher ist α algebraisch über K. □

Satz 1.3.30 (Körperturmsatz)**.** *Für K, L, M Körper und $K \xrightarrow{\iota} L \xrightarrow{\kappa} M$ endliche Körpererweiterungen gilt*

$$[M : K] = [M : L][L : K].$$

Beweis. Sei $\{\alpha_i\}$ eine Basis von L über K und $\{\beta_j\}$ eine Basis von M über L. Wir wollen zeigen, dass $\{\kappa(\alpha_i) \cdot \beta_j\}$ eine Basis für M über K ist.

- (*Erzeugendes System*) Sei $m \in M$ und

  $$m = \sum_{j \in J} \kappa(b_j) \cdot \beta_j, \ b_j \in L$$

  eine Darstellung von m durch die Basis $\{\beta_j\}_{j \in J}$. Gleichwie können wir auch alle b_j-s als Linearkombination der α_i-s darstellen. In anderen Worten, für jeden gegebenen $j \in J$ haben wir

  $$b_j = \sum_{i \in I} a_{ij} \cdot \alpha_i.$$

  Das ergibt (mit Hilfe des Distributivgesetzes und der Tatsache, dass κ ein Ringhomomorphismus ist)

  $$m = \sum_{j \in J} \kappa(b_j) \cdot \beta_j = \sum_{j \in J} \kappa\left(\sum_{i \in I} a_{ij} \cdot \alpha_i\right) \beta_j = \sum_{j \in J} \sum_{i \in I} \kappa\left(a_{ij} \cdot \alpha_i\right) \beta_j = \sum_{i \in I, j \in J} \kappa \circ a_{ij} \cdot \kappa(\alpha_i) \beta_j. \quad (1)$$

- (*Lineare Unabhängigkeit*) Sein $a_{ij} \in K$, so dass

  $$\sum_{i \in I, j \in J} \kappa \circ a_{ij} \cdot \kappa(\alpha_i) \beta_j = 0.$$

Indem wir die obige Notation benutzen und Formel 1 zurückverfolgen haben wir

$$\sum_{i\in I, j\in J} \kappa\circ a_{ij}\cdot\kappa(\alpha_i)\beta_j = \sum_{j\in J}\kappa(b_j)\cdot\beta_j = 0.$$

Da $\{\beta_j\}$ eine Basis von M über L war, folgt, dass $\kappa(b_j) = 0\ \forall j \in J$. Da laut Proposition 1.1.52 der Ringhomomorphismus κ injektiv ist, muss $b_j = 0$, $\forall j \in J$ gelten. Daher $b_j = \sum_{i\in I} a_{ij}\cdot\alpha_i = 0$. Das selbe Argument wie für die b_j-s sagt nun, dass $a_{ij} = 0$ für alle a_{ij}-s.

(Hier ist $\cdot$ nichts als die gewöhnliche Multiplikation in den gegebenen Ringen, die wir als Modulverknüpfung auffassen. Öfters wird dies ausgelassenn. Hier stehen sie es nur zur Klarheit.) □

Korollar 1.3.31. *Sei $[L:K] = n$ und $\alpha \in L$ ein beliebiges Element. Dann sind $[K(\alpha):K] \le n$ und $[L:K(\alpha)] \le n$.*

Bemerkung 1.3.32. Da wir Hauptsächlich mit den Erweiterungen von $\mathbb{Q}$ umgehen werden, sind die Einbettungen kanonisch (es gibt also nur eine Abbildung) $\mathbb{Q} \to L$.

Korollar 1.3.33. *Sei $\iota : K \to L$ eine Körpererweiterung und $L_K^{\mathsf{alg}} \subseteq L$ die Teilmenge der Elemente von L, die algebraisch sind über K. Dann ist L_K^{alg} ein Körper.*

Beweis. Sein $\alpha, \beta \in L_K^{\mathsf{alg}}$. Dann ist β freilich auch algebraisch über $K(\alpha)$, da, wenn es ein Polynom f gibt mit Koeffizienten in K, so dass $f(\beta) = 0$, dann kann man das selbe Polynom auch als ein Element von $K(\alpha)[X]$ auffassen. Aus diesem Grund ist auch $[K(\alpha,\beta):K(\alpha)] \le [K(\beta):K]$, laut unserer Annahme ist $[K(\alpha):K] < \infty$ und daher impliziert der Körperturmsatz 1.3.30, dass auch $[K(\alpha,\beta):K] < \infty$ ist. Sei γ eines der folgenden: $\alpha+\beta, \alpha\beta, \frac{\alpha}{\beta}$ (für das letzte muss $\beta \neq 0$ gelten).

Da $\gamma \in K(\alpha,\beta)$, gilt $K(\gamma) \subseteq K(\alpha,\beta)$. Der Körperturmsatz 1.3.30 besagt nun, dass $[K(\gamma):K]$ endlich sein muss, daher γ algebraisch ist über K. □

Im allgemeinen ist es nicht trivial ein annihilierendes Polynom für die Linearkombination von algebraischen Elementen zu finden.

Beispiel 1.3.34. Sei $K = \mathbb{Q}$, $\alpha = \sqrt{2}, \beta = \sqrt{3}$ und $\gamma = \alpha+\beta = \sqrt{2}+\sqrt{3}$. Es ist unmittelbar, dass $\mathfrak{m}_\alpha = x^2-2$ und $\mathfrak{m}_\beta = x^2-3$. Um γ zu finden, gehen wir wie folgt voran:

Wir haben $\gamma^2 = 5+2\sqrt{6}$ und daher $\gamma^2-5 = 2\sqrt{6}$. Es folgt $(\gamma^2-5)^2-24 = 0 \Rightarrow \gamma^4-10\gamma^2+1 = 0$. Somit ist $f(x) := X^4-10X^2+1$ ein annihilierendes Polynom von γ, das heißt $f(\gamma) = 0$. Mehr als das, $\mathfrak{m}_\gamma = f(x) = X^4-10X^2+1$ ist das Minimalpolynom von γ.

Man kann beweisen, dass das Polynom irreduzibel ist. Sei $f(x) = \mathfrak{m}_\gamma(x) = g(x)h(x)$. Wenn $\mathsf{grad}(g) = 2$ folgt:

$$\mathfrak{m}_\gamma(x) = \left(x^2+ax+b\right)\left(x^2+cx+d\right), \quad a,b,c,d \in \mathbb{Z}.$$

Durchs ausmultiplizieren und vergleichen der Koeffizienten erhalten wir

$$a+c = 0, \quad ac+b+d = -10, \quad ad+bc = 0, \quad bd = 1.$$

Die erste und vierte Gleichung liefert $a = -c$ und $b = d = \pm 1$. Daher ergibt das zweite $a^2 = 10 \pm 2$. Da weder 8 noch 12 eine Quadratzahl in $\mathbb{Z}$ ist, folgt, dass $\mathsf{grad}(g) = 2$ nicht möglich ist.

Wir können so ähnlich auch $\mathsf{grad}(g) = 1$ widerlegen. Einfacher aber ist es, das Lemma von Gauß 1.4.11 und dessen Korollar 1.4.12 zu benutzen, dass wir in kürze zeigen werden. Daraus folgt nämlich, dass ein Linearfaktor von $f(x)$, wenn es existiert, von der Form $X-a$ gewählt werden kann. Das Korollar sagt nun, dass a ein Teiler von 1, also ± 1 sein muss. Da $f(1) \neq 0$, $f(-1) \neq 0$, folgt, dass $\mathsf{grad}(g) = 1$ auch nicht möglich ist. Also ist $f(x) = \mathfrak{m}_\gamma$ irreduzibel, offensichtlich normiert und $\mathfrak{m}_\gamma(\gamma) = 0$, daher das Minimalpolynom von γ.

Eine andere Möglichkeit ist zu beweisen, dass $\sqrt{2} \in \mathbb{Q}(\gamma)$. Daraus wird direkt folgen, dass auch $\sqrt{3} = \gamma - \sqrt{2} \in \mathbb{Q}(\gamma)$. Hierzu gehen wir wie folgt vor: Es gilt

$$\left(\sqrt{2}+\sqrt{3}\right)^2 = 2+2\sqrt{2}\sqrt{3}+3 = 5+\sqrt{6},$$

woraus $\sqrt{6} \in \mathbb{Q}(\gamma)$ folgt. Als solches haben wir auch

$$\left(\sqrt{2} + \sqrt{3}\right)\sqrt{6} = 2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(\gamma).$$

Da aber natürlich $\sqrt{2} + \sqrt{3} = \gamma \in \mathbb{Q}(\gamma)$, ist auch $2\gamma \in \mathbb{Q}(\gamma)$. Es folgt, dass

$$\sqrt{2} = 2\sqrt{3} + 3\sqrt{2} - 2\left(\sqrt{2} + \sqrt{3}\right) \in \mathbb{Q}(\gamma)$$

und wir sind fertig.

Aufgaben

Aufgaben 3

Aufgabe 20 (1 Punkt). Sei $K \to L$ eine Körpererweiterung und $\alpha \in L$. Beweise, dass es genau dann eine Isomorphie

$$K[X] \to K[\alpha]$$

von Ringen gibt, wenn α *nicht* algebraisch über K ist.

Aufgabe 21. [1 Punkt] Sei K ein Körper. Beweise, dass $\{1, X, X^2, \dots, X^{d-1}\}$ eine K-Basis von $K[X]/f(x)$, für jeden irreduziblen Polynom $f(x) \in K[X]$ von Grad d definiert.

Aufgabe 22 (4 Punkte insgesamt). Sei $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ das Körper mit 2 Elementen.

1. (1 Teilpunkt) Beweise, dass $f(x) = x^2 + x + 1$ irreduzibel ist über $\mathbb{F}_2$ und schlussfolgere, dass es einen Körper mit 4 Elementen gibt.
2. (1 Teilpunkt) Wenn wir diesen Körper mit Elementen der Form $(a, b), a, b \in \mathbb{F}_2$ gleichsetzen, gebt die Formel für
$$(a, b) + (c, d)$$
und
$$(a, b)(c, d).$$
3. (2 Teilpunkt) Beweise, dass $x^3 + x + 1$ und $x^3 + x^2 + 1$ irreduzibel sind über $\mathbb{F}_2$. Sind die korrespondierenden Körper mit 8 Elementen isomorph?

Aufgabe 23 (2 Punkte). Sei $0 \neq R$ ein endlicher Integritätsbereich, ungleich dem Nullring. Das heißt, $|R| < \infty$. Beweise, dass R ein Körper ist.

Aufgabe 24 (4 Punkte insgesamt). Sei $\mathbb{Q} \to \mathbb{C}$ eine Körpererweiterung. Finde die Minimalpolynome (über $\mathbb{Q}$) zu den folgenden Elementen (in $\mathbb{C}$).

1. (2 Teilpunkt) $\frac{1+\sqrt{5}}{2}$.
3. (2 Teilpunkt) $\cos(\frac{2\pi}{5})$. (*Tipp: Hier kann man folgende Gleichung benutzen:)*
$$\cos(5\theta) = \cos^5(\theta) - 10\cos^3(\theta)\sin^2(\theta) + 5\cos(\theta)\sin^4(\theta) = 16\cos^5(\theta) - 20\cos^3(\theta) + 5\cos(\theta).$$

Aufgabe 25 (5 Punkte insgesamt). Sei $\alpha = \sqrt{5} + \sqrt{6}$ und sei $L = \mathbb{Q}(\alpha)$.

1. (2 Teilpunkte) Finde das Minimalpolynom von α über $\mathbb{Q}$.
2. (0,5 Teilpunkt) Beweise, dass $\sqrt{30} \in L$.

Sei $K = \mathbb{Q}(\sqrt{30})$.

3. (0,5 Teilpunkt) Finde die Grade der Erweiterungen
$$[K : \mathbb{Q}], [L : K] \text{ und } [L : \mathbb{Q}].$$
4. (1 Teilpunkt) Finde das Minimalpolynom von α über K.
5. (1 Teilpunkt) Beweise, dass $L \simeq \mathbb{Q}(\sqrt{5}, \sqrt{6})$.

Aufgabe 26 (2 Punkte). Finde das Minimalpolynom von $\frac{1+i}{\sqrt{2}}$ über $\mathbb{Q}$. Was sind die anderen Wurzeln dieses Polynoms?

Aufgabe 27 (1 Punkt). Sei R ein Ring. Kann es mehr als einen Elementen $x \in R$ geben, so dass
$$2x = 1?$$

1.4 Polynome über $\mathbb{Z}[X], \mathbb{Q}[X]$ und das Lemma von Gauß

1.4.1 Primitive Polynome

Definition 1.4.1. Sei $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[X]$ ein Polynom über die ganzen Zahlen. Wir sagen, dass die Koeffizienten $\{a_i\}_{i=0}^n$ von f *teilerfremd* sind wenn das Ideal mit ihnen erzeugt ganz $\mathbb{Z}$ ergibt. In anderen Worten, wenn

$$(a_0, a_1, \ldots, a_n) = (1) = Z.$$

Bemerkung 1.4.2. Wenn das Polynom mindestens zwei Koeffizienten ungleich null hat, ist der Begriff recht klar. Wenn das Polynom allerdings nur einen Koeffizienten hat, muss das Koeffizient eine Einheit, also ±1 sein. Z.B., die Koeffizienten von $f(x) = 7x + 2$ sind teilerfremd, *aber die von* $f(x) = 7x$ *sind nicht.*

Definition 1.4.3. Ein Polynom $f \in \mathbb{Z}[X]$ heißt *primitiv* wenn

- die Koeffizienten von f teilerfremd sind und
- der Leitkoeffizient positiv ist.

Lemma 1.4.4. *Sein $\alpha(x), \beta(x) \in \mathbb{Z}[X]$ primitive Polynome, so dass $\alpha(x) = r\beta(x), r \in \mathbb{Q}$. Dann gilt $\alpha(x) = \beta(x)$ und $r = 1$.*

Beweis. Sein $\{a_i\}_{i=0}^n$ die Koeffizienten von $\alpha(x)$, $\{b_j\}_{i=0}^m$ die Koeffizienten von $\beta(x)$ und $r = \frac{c}{d}$, $c, d \in \mathbb{Z}$. Von der Definition der Primitivität folgt, dass $(1) = (a_0, a_1, \ldots, a_n) = (\frac{c}{d}b_0, \frac{c}{d}b_1, \ldots, \frac{c}{d}b_m)$, woraus

$$(d) = (d)(1) = (d)(a_0, \ldots, a_n) = (c)(b_0, \ldots, b_m) = (c)(1) = (c)$$

folgt. In $\mathbb{Z}$ impliziert dies $c = \pm d$, woraus $r = \pm 1$ folgt. Da die Leitkoeffizienten von α und β positiv sind, muss $r = 1$ und $\alpha(x) = \beta(x)$ gelten. □

Proposition 1.4.5. *Sei $0 \neq f \in \mathbb{Q}[X]$ ein Polynom über die rationalen Zahlen. Es gibt ein eindeutiges primitives Polynom $f_p \in \mathbb{Z}[X]$, welches man durch das multiplizieren von f mit einer rationalen Zahl $0 \neq c \in \mathbb{Q}$ erhält.*

Beweis. Der Beweis wird durch Konstruktion gegeben: Wir multiplizieren f mit dem (kleinsten) gemeinsamen Vielfachen c_0 der Nenner der Koeffizienten $\{a_n\}$. Wir multiplizieren dann mit ±1 um eine positive Zahl als Leitkoeffizient zu erhalten. Danach teilen wir die neuen Koeffizienten $\{b_i\}$ durch deren größten gemeinsamen Teiler c_1. Also, wir multiplizieren f mit $c := \pm\frac{c_0}{c_1} \neq 0$.

Es ist nun klar, dass $f_p := cf$ primitiv ist. Eindeutigkeit folgt von Lemma 1.4.4, denn sein $u, v \in \mathbb{Q}$, so dass uf und vf beide primitiv sind. Da $uf = \frac{u}{v}vf$ muss $\frac{u}{v} = 1$ und als solches $u = v$ sein. □

Beispiel 1.4.6. Sei

$$f(x) = -4x^2 + \frac{2}{3}x + 10.$$

Die Nenner sind $(1, 3, 1)$, mit kleinstem gemeinem Vielfachen $c_0 = 3$. Wir erhalten

$$3f(x) = -12x^2 + 2x + 30.$$

Da Ihr Leitkoeffizient negativ ist, multiplizieren wir mit -1. Der größter gemeinsamer Teiler ist $c_1 = 2$ was uns

$$f_p(x) := \frac{-3f(x)}{2} = -\frac{3}{2}f(x) = 6x^2 - x - 15$$

als den eindeutig assoziierten primitiven Polynomial von f liefert.

Es gilt $(\mathbb{Z}/p\mathbb{Z})[X] \simeq \mathbb{Z}[X]/p\mathbb{Z}$. Daher können wir Polynome über $\mathbb{Z}$ zu Polynome über $\mathbb{F}_p$ reduzieren.

Beispiel 1.4.7. Das Polynom $f(x) = 7x^2 + 3x + 2 \in Z[X]$ wird auf $\overline{f}(x) = x^2 + 2 \in \mathbb{F}_3[X]$ projiziert.

Lemma 1.4.8. *Ein Polynom $f(x) \in \mathbb{Z}[X]$ mit positivem Leitkoeffizient is primitiv genau dann wenn $\overline{f} \neq 0 \in \mathbb{F}_p$ für jede Primzahl $p \in Z$.*

Beweis. Sei $\overline{f}(x) = 0 \in \mathbb{F}_p$ für eine gegebene Primzahl p. $\Leftrightarrow$ p teilt all Koeffizienten a_i des Polynoms $f(x)$. $\Leftrightarrow$ $(a_0, a_1, \ldots, a_n) \subseteq (p) \neq (1)$. □

Lemma 1.4.9. *Die primitiven Polynome über $\mathbb{Z}$ formen einen kommutativen Monoid unter der Multiplikation.*

Beweis. Sein $f(x), g(x) \in \mathbb{Z}[X]$, so dass $f(x)g(x)$ nicht primitiv ist. Als solches gibt es eine Primzahl p, welches alle Koeffizienten $\{c_i\}$ von $f(x)g(x)$ teilt. Es folgt, dass $f(x)g(x) = 0 \in \mathbb{F}_p[X]$. Da $\mathbb{F}_p$ ein Körper und daher ein Integritätsbereich ist, gilt $f(x) = 0$ oder $g(x) = 0$ in $\mathbb{F}_p[X]$. Es folgt, dass p alle Koeffizienten von f oder g teilt und daher kann f oder g nicht primitiv sein.

Die Einheit ist natürlich $1 \in \mathbb{Z}[X]$. Kommutativität ist klar und folgt aus der Kommutativität von $\mathbb{Z}[X]$. □

Bemerkung 1.4.10. Die normierten Polynome formen einen Untermonoid des Monoids der primitiven Polynome.

Satz 1.4.11 (Das Lemma von Gauß)**.** *Es sein $f(x), g(x), h(x) \in \mathbb{Q}[X]$ mit*

$$f(x) = g(x)h(x).$$

Dann gilt

$$f_p(x) = g_p(x)h_p(x).$$

Beweis. Sein $a, b, c \in \mathbb{Q}$, so dass $f_p(x) = af(x)$, $g_p(x) = bg(x)$ und $h_p(x) = ch(x)$.

$$\Rightarrow f(x) = \frac{1}{a} f_p(x), g(x) = \frac{1}{b} g_p(x) \quad \text{und} \quad h(x) = \frac{1}{c} h_p(x).$$

$$\Rightarrow \frac{1}{a} f_p(x) = \frac{1}{b} g_p(x) \frac{1}{c} h_p(x)$$

$$\Rightarrow f_p(x) = \frac{a}{bc} g_p(x) h_p(x).$$

Es bleibt zu zeigen, dass $\frac{a}{bc} = 1$. Dies folgt aus Lemma 1.4.4, da sowohl $\alpha(x) := f_p(x)$ (Lemma 1.4.9) wie auch $\beta(x) := g_p(x)h_p(x)$ primitiv sind. □

Als direktes Korollar folgt, dass wenn $f(x) \in \mathbb{Z}[X]$ über $\mathbb{Z}$ irreduzibel ist, es auch über $\mathbb{Q}$ irreduzibel ist.

1.4.2 Weitere Tricks für Polynomzerlegungen

Korollar 1.4.12. *Sei $f(x) \in \mathbb{Z}[X]$ von der Form*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

mit $a_n \neq 0$. Sei $\frac{r}{s} \in \mathbb{Q}$ ein gekürzter Bruch, so dass $f\left(\frac{r}{s}\right) = 0$. Dann gilt $r | a_0$ und $s | a_n$.

Beweis. Die Aussage, dass $\frac{r}{s}$ eine Nullstelle von $f(x)$ ist, ist äquivalent zu sagen, dass

$$f(x) = \left(x - \frac{r}{s}\right) g(x)$$

in $\mathbb{Q}[X]$. Daher gibt es $b, c \in \mathbb{Q}$, so dass $b\left(x - \frac{r}{s}\right)$ und $cg(x)$ in $\mathbb{Z}[X]$ liegen und

$$f(x) = b\left(x - \frac{r}{s}\right) cg(x).$$

Wir können nicht direkt annehmen, dass $b, c \in \mathbb{Z}$, da wir immer noch f faktorisieren wollen, nicht bcf. Jedoch gilt $b, \frac{br}{s} \in \mathbb{Z}$ weil $b\left(x - \frac{r}{s}\right) \in \mathbb{Z}[X]$. Aus r, s teilerfremd (gekürzt), folgt $s|b$. Da b das Leitkoeffizient von $b\left(x - \frac{r}{s}\right)$ ist, muss es den Leitkoeffizienten von $f(x)$ teilen, was a_n ist. Also, $s|b \;\;\&\;\; b|a_n \Rightarrow s|a_n$.

Gleichwie muss $\frac{br}{s}$ den Konstanten Term von $f(x)$, also a_0 teilen. Da $b|s$ ist gilt $\frac{b}{s} \in \mathbb{Z}$, also $\frac{br}{s} = \frac{b}{s}r$, also $r|a_0$, da $\frac{b}{s}r \mid a_0$. □

Korollar 1.4.13. *Sei $f(x) \in \mathbb{Z}[X]$ ein normiertes Polynom mit einer rationalen Wurzel $\alpha \in \mathbb{Q}$. Dann ist $\alpha \in \mathbb{Z}$ eine ganze Zahl die den freien Term von $f(x)$ teilt und es gilt*

$$f(x) = (x - \alpha)g(x)$$

wobei $g(x)$ selber normiert ist.

Beweis. Dies ist ein direktes Korollar von 1.4.12, wobei $g(x)$ normiert ist, da das Leitkoeffizient von $f(x)$ gleich dem Produkt der Leitkoeffizienten von $(x - a)$ und $g(x)$ ist. □

Korollar 1.4.14. *Sei $f(x) \in \mathbb{Z}[X]$ ein normiertes Polynom mit $\mathsf{grad}(f) \leq 3$, welches reduzibel ist über $\mathbb{Q}$. Dann hat $f(x)$ eine Wurzel über $\mathbb{Z}$, welches ein Teiler des freien Terms ist.*

Als solches reicht es für normierte Polynome vom Grad ≤ 3 aus, die Teiler des freien Terms zu überprüfen, wenn man nach Lösungen über $\mathbb{Z}$ sucht.

Beispiel 1.4.15. Das Polynom $f(x) = x^3 + x + 1$ ist irreduzibel über $\mathbb{Q}$ da $f(1)$ und $f(-1)$ nicht Null werden.

Die folgende Überlegung ist zwar "trivial", aber eines der effektivsten Methoden die Irreduzibilität eines Polynoms über $\mathbb{Z}$ (und daher auch über $\mathbb{Q}$ durch das Lemma von Gauß 1.4.11) zu beweisen:

Proposition 1.4.16. *Sei $f(x) \in \mathbb{Z}[X]$. Wenn es eine Primzahl $p \in \mathbb{Z}$ gibt welches den Leitkoeffizienten von f nicht teilt und für der $\overline{f(x)} \in \mathbb{F}_p[X] = \mathbb{Z}/p\mathbb{Z}[X]$ irreduzibel über $\mathbb{F}_p$ ist, dann ist $f(x)$ irreduzibel über $\mathbb{Z}$.*

Beweis. Sei $f = gh$ eine Zerlegung über $\mathbb{Z}$, mit a_n, b_m, c_k Leitkoeffizienten von f, g, h, so dass $\mathsf{grad}(g) = m, \mathsf{grad}(h) = k \geq 1$. Dann gilt $\overline{f} = \overline{g}\overline{h}$ über $\mathbb{F}_p$. Da $p \nmid a_n$ folgt $p \nmid b_m, p \nmid c_k$, was $\mathsf{grad}(\overline{g}) = \mathsf{grad}(g) \geq 1$ und $\mathsf{grad}(\overline{h}) = \mathsf{grad}(h) \geq 1$ impliziert. Es folgt, dass aus f reduzibel über $\mathbb{Z}$, $\overline{f}$ reduzibel über $\mathbb{F}_p$ ist. Die Umkehrung ist unsere Aussage. □

Beispiel 1.4.17. Das Polynom $f(x) = x^4 + x^3 + 1$ ist irreduzibel über $\mathbb{Q}[X]$, da $\overline{f}(x)$ irreduzibel über $\mathbb{Z}/2\mathbb{Z}$ ist. Daraus kann man auch direkt schließen, dass $g(x) = 3x^4 + 7x^3 + 2x + 17$ auch irreduzibel ist, da $\overline{f}(x) = \overline{g}(x)$ über $\mathbb{F}_2$ und 2 auch den Leitkoeffizienten von g nicht teilt. Man könnte es aber *nicht* für $h(x) = 2x^5 + x^4 + x^3 + 1$ folgern.

Satz 1.4.18 (Eisensteins Kriterium)**.** *Sei $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[X]$ primitiv und $p \in \mathbb{Z}$ eine Primzahl die folgendes erfüllt:*

- $p \mid a_i$, $1 \leq i \leq n - 1$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$.

Dann ist $f(x)$ irreduzibel über $\mathbb{Z}$ (und daher auch über $\mathbb{Q}$).

Beweis. Sei $f(x) = g(x)h(x)$, $g(x), h(x) \in \mathbb{Z}[X]$, mit b_m und c_k als Leitkoeffizienten von $g(x)$ und $h(x)$. Dann gilt auch $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ in $\mathbb{Z}/p\mathbb{Z}$, wobei p die Primzahl der Aussage ist. Bei Annahme ist das Leitkoeffizient $\overline{a}_n$ das einzige Koeffizient von $\overline{f}(x)$ welches ungleich Null ist. Also, $\overline{f}(x) = \overline{a}_n x^n$.

Da $\mathbb{Z}/p\mathbb{Z}$ ein Körper und daher ein Integritätsbereich ist, folgt, dass $\overline{g}(x) = \overline{b}_m x^m$ und $\overline{h}(x) = \overline{c}_k x^k$, mit $n, m, k \in \mathbb{N}$ und $m + k = n$. (Wenn es nicht klar ist, überlege man sich, was passiert, wenn eines der Polynome mehr als einen Summanden hat. Dann wird das Produkt auch mehr als einen haben müssen. Des weiteren muss $\overline{b}_m$ und $\overline{c}_k$ von den Leitkoeffizienten kommen, sonst wird $m + k = n$ in $\mathbb{F}_p$ nicht mehr gelten.)

Wenn $m, k \geq 1$, folgt, dass $\overline{g}(x)$ und $\overline{h}(x)$ beide keine konstanten Terme haben. Also, dass die konstante Terme von $g(x)$ und $h(x)$, beide, durch p teilbar sind. Daraus würde folgen, dass das konstante Term von $f(x)$ durch p^2 teilbar wäre, was ein Widerspruch zur Annahme ist.

Daher ist $m = 0$ oder $k = 0$, also ist $g(x)$ oder $h(x)$ eine konstante Funktion. Primitivität von $f(x)$ impliziert nun, dass $g(x) = \pm 1$ oder $h(x) = \pm 1$. □

Beispiel 1.4.19. Das Polynom $f(x) = 8x^7 + 14x^5 + 21$ ist irreduzibel über $\mathbb{Q}[X]$ aus Eisensteins Kriterium für $p = 7$.

Proposition 1.4.20. *Ein Polynom $f(x) \in K[X]$ ist genau dann irreduzibel, wenn $f(x+a), a \in K$ irreduzibel ist.*

Beweis. Aufgabe 28. □

Aufgaben

Aufgaben 4

Aufgabe 28 (1 Punkt). Sei $f(x) \in K[X]$ ein Polynom. Beweise, dass es genau dann irreduzibel ist, wenn $f(x+a), a \in K$ irreduzibel ist.

Aufgabe 29 (2 Punkte). Beweise mithilfe von Eisensteins Kriterium, dass folgende Polynome irreduzibel sind:

(i) $x^4 + 2x^3 + 2x + 2$

(ii) $x^4 + 9$.

Aufgabe 30 (3 Punkte). *Kreisteilungspolynome* bzw. *zyklotomische Polynome* sind die irreduziblen Teiler des Polynoms $x^n - 1 \in \mathbb{Z}[X]$. Diese werden mit Φ_n bezeichnet. Für den Fall $n = p$ Primzahl, sind diese besonders einfach (und wichtig). Basierend auf die vorige Aufgabe 28, beweise, dass

$$\Phi_p := x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1.$$

Also, dass das obige Polynom $(1 + x + \cdots + x^{p-1})$ irreduzibel ist und ein Teiler von $x^p - 1$.

Aufgabe 31 (4 Punkte). Finde alle reduziblen Polynome (über $\mathbb{Q}$) der Form

$$t^5 + at^3 + bt + 1,$$

wobei $a, b \in \mathbb{Z}$.

Aufgabe 32 (2 Punkte). Ist das Polynom

$$x^6 + 7x^5 + 2x^2 + 18x + 28$$

irreduzibel? Wenn ja, beweise. Wenn nicht, faktorisiere es in irreduzible Komponente.

Aufgabe 33 (2 Punkte). Sei $f(x) = a_0 + a_1 x + \cdots + a_{n_1} x^{n-1} + a_n x^n$ irreduzibel. Beweise, dass auch $g(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$ irreduzibel ist. (*Tipp*: Man schreibe $g(x) = x^n f\left(\frac{1}{x}\right)$.)

1.5 Symmetrische Polynome

Definition 1.5.1. Ein Polynom $S(x_1, x_2, \ldots, x_n)$ in n Variablen heißt symmetrisch, wenn für alle Permutationen $\sigma_i \in \Sigma_n$ gilt

$$S(x_1, x_2, \ldots, x_n) = S(\sigma_i(x_1, x_2, \ldots, x_n)).$$

Wir werden die Menge aller symmetrischen Polynome in n Variablen mit $\mathsf{Sym}_n(K)$ bezeichnen.

Beispiel 1.5.2. Die folgenden Polynome sind symmetrisch:

- $x \in K[X]$;
- $x^2 + y^2 \in K[X, Y]$;
- $xy^2 + x^2y + x + y \in K[X, Y]$;
- $xy^2z^3 + xy^3z^2 + x^2yz^3 + x^2y^3z + x^3yz^2 + x^3y^2z \in K[X, Y, Z]$;

Die folgenden Polynome sind *nicht* symmetrisch:

- $x^2y \in K[X, Y]$;
- $x + y + xyz \in K[X, Y, Z]$.

Ob ein Polynom symmetrisch ist hängt davon ab, in welchem Polynomring wir sind:

- x ist symmetrisch in $K[X]$, aber x ist *nicht* symmetrisch in $K[X, Y]$.

Elementare symmetrische Polynome Besonders wichtige Typen von symmetrischen Polynomen in $K[X_1, \ldots, X_n]$ sind

$$\begin{aligned}
s_1 &:= x_1 + \cdots + x_n = \sum_{i=1}^{n} x_i \\
s_2 &:= x_1x_1 + x_1x_3 + \cdots + x_{n-1}x_n = \sum_{1 \le i < j \le n} x_ix_j \\
s_3 &:= x_1x_2x_3 + \cdots + x_{n-2}x_{n-1}x_n = \sum_{1 \le i < j < k \le n} x_ix_jx_k \\
&\vdots \\
s_n &:= x_1x_2 \ldots x_n.
\end{aligned}$$

Diese werden *elementare symmetrische Polynome* genannt. Wie wir bald sehen werden, kann jedes symmetrische Polynom als eine polynomiale Kombination von symmetrischen Polynomen dargestellt werden.

Obwohl symmetrische Polynome fast schon bei Definition viele Variablen enthalten müssen (in einer Variable ist jedes Polynom symmetrisch), werden wir sehen, dass diese trotzdem sehr nützlich für Polynome mit einer Variable sind. Die Ideen, die wir in diesem Kapitel sehen werden sind in vielerlei Hinsicht die Anfänge von Galois Theorie.

Sei

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x_n \in K[X] \tag{2}$$

ein normiertes Polynom über einen Körper K in einer Variable x. Sei $\hat{K}$ der algebraische Abschluss von K. Jeder Körper hat so einen Abschluss (welches Eindeutig bis zur Isomorphie ist). Jedoch kann man hier auch einen größeren algebraisch abgeschlossenen Körper nehmen. Z.B., kann man bei $\mathbb{Q}$ auch $\mathbb{C}$ nehmen, obwohl $\hat{\mathbb{Q}} \subsetneq \mathbb{C}$.

Über $\hat{K}$ kann man $f(x)$ schreiben als

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i),$$

wobei einige der α_i-s gleich sein können. Wenn wir ausmultiplizieren und umordnen erhalten wir

$$f(x) = (-1)^n s_n(\alpha) + \cdots - s_1(\alpha)x^{n-1} + x^n, \tag{3}$$

wobei die s_i's die elementaren symmetrischen Polynome sind. Diese sind Polynome in n Variablen und wir benutzen die Notation $s_i(\alpha)$ als Kurzform von $s_i(\alpha_1, \ldots, \alpha_n)$. Wenn wir nun die Gleichungen 2 und 3 gleichsetzen, erhalten wir

$$\begin{aligned} a_0 &= (-1)^n s_n(\alpha) && (4)\\ a_1 &= (-1)^{n-1} s_{n-1}(\alpha) && (5)\\ &\vdots && (6)\\ a_{n-2} &= s_2(\alpha) && (7)\\ a_{n-1} &= -s_1(\alpha). && (8) \end{aligned}$$

In anderen Worten, obwohl es im allgemeinen sehr schwer ist die Wurzeln von Polynomen zu finden, sind deren (elementare) symmetrische Kombinationen trivial von den Koeffizienten abzulesen.

Beispiel 1.5.3. Lass uns den quadratischen und kubischen Fall in Detail anschauen:

- Sei $f(x) = a_0 + a_1 x + x^2$ und lass α_1, α_2 die Wurzeln von $f(x)$ in $\hat{K}$ sein. ($\alpha_1 = \alpha_2$ ist natürlich erlaubt.) Dann können wir $f(x)$ als

  $$f(x) = (x - \alpha_1)(x - \alpha_2) = \alpha_1\alpha_2 - (\alpha_1 + \alpha_2)x + x^2$$

  schreiben. Daher sind

  $$\begin{aligned} a_0 &= (-1)^2 s_2(\alpha) = s_2(\alpha_1, \alpha_2) = \alpha_1\alpha_2,\\ a_1 &= (-1)^1 s_1(\alpha) = -s_1(\alpha_1, \alpha_2) = -(\alpha_1 + \alpha_2). \end{aligned}$$

- Sei $f(x) = a_0 + a_1 x + a_2 x^2 + x^3$ und lass $\alpha_1, \alpha_2, \alpha_3$ die Wurzeln von $f(x)$ in $\hat{K}$ sein. Dann können wir $f(x)$ als

  $$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = -(\alpha_1\alpha_2\alpha_3) + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + x^3$$

  schreiben, was uns

  $$\begin{aligned} a_0 &= (-1)^3 s_3(\alpha) = -s_3(\alpha_1, \alpha_2, \alpha_3) = -\alpha_1\alpha_2\alpha_3,\\ a_1 &= (-1)^2 s_2(\alpha) = s_2(\alpha_1, \alpha_2, \alpha_3) = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3,\\ a_2 &= (-1)^1 s_1(\alpha) = -s_1(\alpha_1, \alpha_2, \alpha_3) = -(\alpha_1 + \alpha_2 + \alpha_3) \end{aligned}$$

  gibt.

1.5.1 Der Satz von Newton

Proposition 1.5.4. *Sei $K[X_1, \cdots, X_n]$ das Ring der Polynome in n Variablen über einen Körper K. Die symmetrischen Polynome $\mathsf{Sym}_n(K)$ bilden einen kommutativen Unterring (K-Algebra) von $K[X_1, \cdots, X_n]$.*

Beweis. Es ist klar, dass $0, 1 \in \mathsf{Sym}_n(K)$ (jede Konstante ist symmetrisch). Sein $f, g \in K[X_1, \ldots, X_n]$ symmetrisch. Dann gilt bei Definition von $(f + g)(x_1, \ldots, x_n)$ und $(fg)(x_1, \ldots, x_n)$, dass

$$\begin{aligned} (f + g)(x_1, \ldots, x_n) &= f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n)\\ &= f(\sigma(x_1, \ldots, x_n)) + g(\sigma(x_1, \ldots, x_n)) = (f + g)(\sigma(x_1, \ldots, x_n)) \end{aligned}$$

und

$$\begin{aligned} (fg)(x_1, \ldots, x_n) &= f(x_1, \ldots, x_n)g(x_1, \ldots, x_n)\\ &= f(\sigma(x_1, \ldots, x_n))g(\sigma(x_1, \ldots, x_n)) = (fg)(\sigma(x_1, \ldots, x_n)), \end{aligned}$$

für eine beliebige Permutation $\sigma \in \Sigma_n$.

(Um zu überprüfen, dass es auch ein K-Algebra ist, muss man zusätzlich noch zeigen, dass $\mathsf{Sym}_n(K)$ ein K-Modul ist wo $k(fg) = (kf)g$, für alle $k \in K, f, g \in \mathsf{Sym}_n(K)$. Aber, da $\mathsf{Sym}_n(K) \subseteq K[X_1, \ldots, X_n]$ und ein Unterring eines K-Algebras automatisch ein K-Algebra ist, erübrigt sich dies. □

Bemerkung 1.5.5. Wie schon angesprochen werden wir Module und K-Algebren nicht in diesem Kurs benötigen. Wir werden es nur ab-und-zu erwähnen für die, die es schon kennen.

Lexikographische Ordnung Ehe wir den nächsten Satz beweisen können, müssen wir eine Definitionen einführen:

Definition 1.5.6. Sein $x_1^{a_1} \cdots x_n^{a_n}$ und $x_1^{b_1} \cdots x_n^{b_n}$ zwei Monomiale. Wir sagen

$$x_1^{a_1} \cdots x_n^{a_n} > x_1^{b_1} \cdots x_n^{b_n}$$

genau dann wenn

- $a_1 > b_1$; oder
- $a_1 = b_1$ und $a_2 > b_2$; oder
- $a_1 = b_1$, $a_2 = b_2$ und $a_2 > b_2$; oder
- $\vdots$.

Dies wird die *lexikographische Ordnung* genant.

In anderen Worten, wir führen zuerst eine Ordnung auf die Variablen ein, wo wir sagen $x_1 > x_2 > \cdots$ und dies induziert dann die gegebene Ordnung. Diese Ordnung kennt man vor allem bei der Olympiade, wo man zuerst die Anzahl der Goldmedaillen zählt, dann Silber und schließlich Bronze.

Es ist natürlich hochgradig nicht kanonisch. Man könnte auch $x_2 > x_1 > x_3$ sagen. Wenn die Variablen z.B., A, α, X_1 heißen, sieht man, dass es keine "universelle" Ordnung gibt. Man wählt sich schlicht und einfach eine aus.

Beispiel 1.5.7. Sei $x_1 > x_2 > x_3$. Wir haben

- $x_1 x_2 > x_1$;
- $x_1 x_2 > x_1 x_3$;
- $x_1^2 x_2 x_3 > x_1 x_2^2 x_3^3$;
- $x_1^2 > x_1 x_2^2 x_3$;
- Die Monomiale x_1 und $2x_1$ sind nicht vergleichbar.

Bemerkung 1.5.8. Der Grund, warum wir die Koeffizienten beim Vergleich nicht mit einbeziehen ist, dass es in allgemeinen Körpern (einschließlich denen die wir brauchen) keine Ordnung gibt. Z.B. gibt es keine Ordnung in $\mathbb{Q}(i)$.

Sei $f(x_1, \ldots, x_n)$ ein Polynom in n Variablen. Dann führt die lexikographische Ordnung eine Ordnung auf die Monomiale von $f(x_1, \ldots, x_n)$ ein.

Definition 1.5.9. Das *Leitmonomial* von $f(x_1, \ldots, x_n)$ ist definiert als das größte Monomial unter der lexikographischen Ordnung.

Beispiel 1.5.10. Das Leitmonomial von

$$f(x_1, x_2, x_3) = 5x_1^5 x_2 + 7x_1 x_2^7 x_3^5$$

ist $5x_1^2 x_2$.

Definition 1.5.11. Sein $f(x_1,\dots,x_n)$ und $g(x_1,\dots,x_n)$ Polynome in n Variablen. Wir sagen

$$f(x_1,\dots,x_n) \ > \ g(x_1,\dots,x_n)$$

wenn das Leitmonomial von f lexikographisch größer als das Leitmonomial von g ist.

Bemerkung 1.5.12. Hier könnte man eigentlich weitermachen und sagen, wenn die Leitmonomiale gleich sind, vergleiche die zweitgrößten Monomiale. (Also, schmeiße die Leitmonomiale weg und definiere so $f^{\#}$ und $g^{\#}$, und vergleiche nun die neuen Leitmonomiale). Wir werden all das aber nicht für unseren Beweis brauchen.

Beispiel 1.5.13. Sei $x_1 \ > \ x_2 \ > \ x_3$.

- Wir haben
$$5x_1^5x_2 + 7x_1x_2^7x_3 \ > \ 8x_1^3x_2^9x_3^7 + 7x_1x_2^2 + x_3$$
da $5x_1^5x_2 \ > \ 8x_1^3x_2^9x_3^7$ in der lexikographischen Ordnung, denn $x_1^5 \ > \ x_1^3$ ist das einzige worauf es hier ankommt.
- Die Polynome
$$f = 5x_1^5x_2 + 7x_1x_2^7x_3 \ \ \& \ \ 5x_1^5x_2 + 7x_1x_2^5x_3^2 + x_2 = g$$
vergleichen wir hier nicht weiter. Man könnte, wie in Bemerkung 1.5.12 angedeutet,
$$f^{\#} = 7x_1x_2^7x_3 \ \ \& \ \ 7x_1x_2^5x_3^2 + x_2 = g^{\#}$$
weiter vergleichen und sagen, da $f^{\#} \ > \ g^{\#} \Rightarrow f \ > \ g$.

Lemma 1.5.14. *Sein $f(x_1,\dots,x_n)$, $g(x_1,\dots,x_n) \in K[X_1,\dots,X_n]$. Dann ist das Leitmonomial von $fg \in K[X_1,\dots,X_n]$ gleich dem Produkt der Leitmonomiale von f und g.*

Beweis. Aufgabe 34. □

Lemma 1.5.15. *Sei $f(x_1,\dots,x_n) \in K[X_1,\dots,X_n]$ ein symmetrisches Polynom. Dann gilt für das Leitmonomial*

$$\lambda x_1^{a_1}\cdots x_n^{a_n},$$

dass $a_1 \geq a_2 \geq \cdots \geq a_n$.

Beweis. Nimm ein Monomial

$$\lambda x_1^{b_1}\cdots x_i^{b_i}\cdots x_j^{b_j}\cdots x_n^{b_n}$$

wo es nicht gilt, also wo es $1 \leq i,j, \leq n$ gibt mit $b_i < b_j, i < j$. Dann muss $f(x_1,\dots,x_n)$ aus Symmetrie auch

$$\lambda x_1^{b_1}\cdots x_i^{b_j}\cdots x_j^{b_i}\cdots x_n^{b_n}$$

erhalten, da wir dies aus der Permutation $(i,j) \in \Sigma_n$ erhalten. Es ist klar, dass das zweite größer ist unter der lexikographischen Ordnung. Daher kann das erste nicht das Leitmonomial sein. □

Satz 1.5.16 (Der Satz von Newton)**.** *Jedes symmetrische Polynom kann als eine eindeutige polynomiale Kombination der elementaren symmetrischen Polynome dargestellt werden.*

Bemerkung 1.5.17. Etwas formeller formuliert heißt es, dass das Ring $\mathsf{Sym}_n(K) \subseteq K[X_1,\dots,X_n]$ (K-Algebra) der symmetrischen Polynome isomorph zu $K[X_1,\dots,X_n]$ ist. Diese Isomorphie wird durch

$$K[X_1,\dots,X_n] \ni f(x_1,\dots,x_n) \mapsto f(s_1,\dots,s_n) \in \mathsf{Sym}_n(M)$$

gegeben. Die Tatsache, dass die Standardeinbettung $\mathsf{Sym}_n(K) \subsetneq K[X_1,\dots,X_n]$ klar nicht surjektiv ist, sollte einen nicht verwirren, da bekanntlich auch $2\mathbb{Z} \subsetneq \mathbb{Z}$, diese aber trotzdem (als abelsche Gruppen) isomorph sind.

Beweis. [Beweis von Satz 1.5.16] Wir werden dies durch Induktion auf die Größe (unter der lexikographischen Ordnung) des Leitmonomials beweisen. Sei $f(x_1, \cdots, x_n)$ ein symmetrisches Polynom, mit Leitmonomial $\lambda x_1^{a_1} \cdots x_n^{a_n}$, wobei $\lambda \in K$ ein Koeffizient ist.

Wir behaupten, dass es $(b_1, \cdots, b_n) \in \mathbb{N}^n$ gibt, so dass das Leitmonomial von $\lambda s_1^{b_1} \cdots s_n^{b_n}$ gleich $\lambda x_1^{a_1} \cdots x_n^{a_n}$ ist (zur Erinnerung, die s_i's sind Polynome, nicht Variablen, sieh Beispiel 1.5.18 zur weiteren Erläuterung).

Um diese Behauptung zu sehen, bemerken wir, dass das Leitmonomial von $s_1^{b_1} \cdots s_n^{b_n}$ gleich

$$x_1^{b_1}(x_1x_2)^{b_2}(x_1x_2x_3)^{b_3} \cdots (x_1 \cdots x_n)^{b_n}$$

ist. Das folgt direkt von Lemma 1.5.14 und der Tatsache, dass das Leitmonomial von s_1 gleich x_1 ist, von s_2 ist es x_1x_2 u.s.w.. Daher suchen wir $b_1, \cdots, b_n$, so dass

$$\begin{aligned} b_1 + \cdots + b_n &= a_1 \\ b_2 + \cdots + b_n &= a_2 \\ &\vdots \\ b_n &= a_n. \end{aligned}$$

Dies hat eine eindeutige Lösung

$$b_i = \begin{cases} a_n & \text{wenn } \ i = n \\ a_i - a_{i+1} & \text{für } i < n. \end{cases}$$

Dies ist Wohldefiniert laut Lemma 1.5.15, da $a_i - a_{i+1} \geq 0$ ist.

Durch unsere Behauptung können wir nun

$$g(x_1, \cdots, x_n) := f(x_1, \cdots, x_n) - \lambda s_1^{b_1} \cdots s_n^{b_n}$$

definieren, wessen Leitmonomial streng kleiner ist (im Sinne der lexikographischen Ordnung) als die von f. Bei der Induktionsannahme kann daher g als eine polynomiale Kombination der elementaren symmetrischen Polynome dargestellt werden, also auch $f = g + \lambda s_1^{b_1} \cdots s_n^{b_n}$. □

Beispiel 1.5.18. Sei $n = 3$. Dann ist

$$s_1^2 s_2^2 s_3 = (x_1 + x_2 + x_3)^2 (x_1x_2 + x_1x_3 + x_2x_3)^2 (x_1x_2x_3)$$

Wenn $x_1 > x_2 > x_3$ ist das Leitmonomial davon

$$x_1^2 (x_1x_2)^2 x_1x_2x_3 = x_1^5 x_2^3 x_3.$$

Eine direkte Implikation von dem Satz von Newton 1.5.16 ist folgendes Korollar:

Korollar 1.5.19. *Sei $f(x) \in K[X]$ und $\{\alpha_1, \ldots, \alpha_n\}$ die Wurzeln von f über $\hat{K}$. Dann ist $S(\alpha_1, \ldots, \alpha_n) \in K$, für jeden symmetrischen Polynom $S \in \mathsf{Sym}_n(K)$ über K.*

Beweis. Laut Newtons Satz ist

$$S = \sum_{j=1}^{k} \lambda_j s_1^{b_{j1}} s_2^{b_{j2}} \cdots s_n^{b_{jn}},$$

eine polynomiale Kombination der elementaren Symmetrischen Polynome. Da die $s_i(\alpha_1, \ldots, \alpha_n)$ die Koeffizienten von f sind (bis auf Vorzeichen), also in K liegen, folgt, dass $S(\alpha_1, \ldots, \alpha_n) \in \hat{K}$. □

Eine weitere und wichtige Implikation ist, dass obwohl die einzelnen Wurzeln eines Polynoms schwer, oder fast unmöglich zum bestimmen sind, sind ihre symmetrischen Kombinationen einfach zu bestimmen. Das heißt, für jeden $S \in \mathsf{Sym}_n(K)$, ist $S(\alpha_1, \ldots, \alpha_n)$ einfach zu finden, auch wenn wir die einzelnen α_i's gar nicht kennen.

Hier sind die $\alpha_i \in \hat{K}$'s die Wurzeln eines Polynoms $f(x) \in K[X]$ über dessen algebraischen Abschluss.

Beispiel 1.5.20. Sei $f(x) = x^2+2x+7$ und $\alpha_1, \alpha_2 \in \mathbb{C}$ die Wurzeln von f. Ohne diese zu bestimmen, können wir direkt sagen, dass

$$\begin{aligned} \alpha_1^2 + \alpha_2^2 &= (\alpha_1 + \alpha_2)^2 - 2\alpha_1\alpha_2 \\ &= s_1^2 - 2s_2 \\ &= (-a_1)^2 - 2a_0 \\ &= 4 - 14 = -10 \end{aligned}$$

Aufgaben

Aufgaben 5

Aufgabe 34 (1 Punkt). Sein $f(x_1,\dots,x_n)$, $g(x_1,\dots,x_n) \in K[X_1,\dots,X_n]$. Zeige, dass das Leitmonomial von $fg \in K[X_1,\dots,X_n]$ gleich dem Produkt der Leitmonomiale von f und g ist.

Aufgabe 35 (4 Punkte). Stelle die folgenden Polynome als polynomiale Kombination der elementaren symmetrischen Polynome dar:

i) $f = x^2 + y^2 + z^2 \in K[X,Y,Z]$

ii) $g = x^2y^2 + x^2z^2 + y^2z^2 \in K[X,Y,Z]$

iii) $h = x^4y^2 + x^2y^4 + x^2y^2z^2 + x^4z^2 + x^2z^2y^2 + x^2z^4 + y^2z^2x^2 + y^4z^2 + y^2z^4 \in K[X,Y,Z]$ (*Tipp: Hier kann man vielleicht etwas vereinfachen...vielleicht auf etwas schon bekanntest beziehen?*)

iv) $i = (x-2y)^2(y-2x)^2 \in K[X,Y]$.

Aufgabe 36 (3 Punkte). Sein $\alpha,\beta,\gamma,\delta \in \mathbb{C}$ die Nullstellen des Polynoms

$$f(x) = x^4 - 2x^3 + 4x^2 - 6.$$

Ohne die Nullstellen zu bestimmen, berechne

- $\alpha^2 + \beta^2 + \gamma^2 + \delta^2$
- $\alpha^2\beta + \alpha^2\gamma + \alpha^2\delta + \alpha\beta^2 + \beta^2\gamma + \beta^2\delta + \alpha\gamma^2 + \beta\gamma^2 + \gamma^2\delta + \alpha\delta^2 + \beta\delta^2 + \beta\delta^2$
- Beweise, dass
$$\alpha^3 + \beta^3 + \gamma^3$$
irrational ist.

Aufgabe 37 (1 Punkt). Sein $\alpha_1,\cdots,\alpha_n$ die Wurzel des Polynoms

$$f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_n.$$

Bestimme die Summe $x_1^2 + \cdots + x_n^2$.

Aufgabe 38 (2 Punkte). Finde λ, so dass eines der Wurzeln von $f(t) = t^3 - 7t + \lambda$, doppelt so groß ist wie eines der Anderen.

2 Algebraische Zahlenkörper

2.1 Körpereinbettungen

Definition 2.1.1. Ein Körper K heißt *Zahlenkörper*, wenn K eine Körpererweiterung von $\mathbb{Q}$ vom endlichen Grad ist. Also $[K:\mathbb{Q}] < \infty$.

Jede endliche (bzw. algebraische) Körpererweiterung von $\mathbb{Q}$ ist ein Unterkörper von $\mathbb{C}$. Daher können auch den 'größten' algebraischen Zahlenkörper definieren: Die Teilmenge $\mathbb{C}^{\mathsf{alg}}_{\mathbb{Q}} \subseteq \mathbb{C}$ "aller" algebraischen Elemente über $\mathbb{Q}$ formen einen Körper nach Korollar 1.3.33. Elemente davon werden *algebraische Zahlen* genannt. Eine andere, und deutlich gängigere, Notation dafür ist $\hat{\mathbb{Q}}$. Wir werden es jetzt nicht zeigen, aber $\mathbb{C}^{\mathsf{alg}}_{\mathbb{Q}} = \hat{\mathbb{Q}}$ ist der algebraische Abschluss von $\mathbb{Q}$. Das heißt, alle Polynome in einer Variable zerfallen in Linearkombinationen/haben einen Wurzel. Nach Hilberts Nullstellensatz gilt auch etwas ähnlicheres für mehrere Variablen - dies ist jedoch Teil der algebraischen Geometrie und wird nicht in diesem Kurs vorkommen.

Satz 2.1.2 (Galoisscher Separablitätssatz)**.** *Sei $K \xrightarrow{\iota} \mathbb{C}$ ein Unterkörper der komplexen Zahlen und $f(x) \in K[X]$ irreduzibel über K. Dann hat f keine doppelten-Wurzeln: Das heißt*

$$f(x) = \prod_{i=1}^{d} (x - \alpha_i),$$

wobei $\alpha_i \in \mathbb{C}$ alle verschieden sind.

Beweis. Sei α eine doppelte Wurzel von $f(x)$. Dann ist $f(x)$ von der Form

$$f(x) = (x-\alpha)^2 g(x).$$

Daher ist die Ableitung

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) = (x-\alpha)\left(2g(x) + (x-\alpha)g'(x)\right).$$

Wir haben, $f'(\alpha) = 0$ und daher $f'(x) \in I(\alpha)$. Sei $0 \neq r \in K$. Es ist klar, dass ein Polynom $h(x)$ eine Nullstelle α hat, genau dann wenn $rh(x)$ die selbe Nullstelle hat: also $h(\alpha) = 0 \Leftrightarrow rh(\alpha) = 0$. Daher können wir annehmen, dass $f(x)$ normiert war. Da f aber irreduzibel ist und $f(\alpha) = 0$, folgt laut Proposition 1.3.14, dass f das Minimalpolynom von α ist, daher besagt Korollar 1.3.8, dass $I(\alpha) = (f)$. Dies ist ein Widerspruch, da $f' \in I(\alpha) = I(f)$ von strikt geringerer Grad ist. □

Da jede algebraische Körpererweiterung von $\mathbb{Q}$ in $\mathbb{C}$ liegt, kann K jedes algebraische Zahlenkörper sein.

Bemerkung 2.1.3. Dieses Argument (und Aussage) ist falsch, wenn wir nicht annehmen, dass $K \subseteq \mathbb{C}$. In Körpern mit Charakteristik p (wo also $p \cdot x = 0 \ \forall x \in K$, z.B., $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$) kann f' null sein, obwohl f eine doppelte Wurzel hat. Z.B., über dem Körper $\mathbb{F}_3$ mit dem Polynom $f(x) = (x-\alpha)^3 \in \mathbb{F}_3[X]$.

Satz 2.1.4. *[Satz vom primitiven Element] Sei L eine endliche Körpererweiterung von K und sei $K \xrightarrow{\iota} L \xrightarrow{\kappa} \mathbb{C}$. Dann gibt es ein Element $\theta \in L$, so dass $L = K(\theta)$.*

Beweis. Da L eine endliche Erweiterung ist und daher endlich dimensional als K-Vektorraum, folgt, dass es endlich viele $\alpha_1, \ldots, \alpha_n$ gibt, mit $L = K(\alpha_1, \ldots, \alpha_n)$. Mithilfe des Induktionsarguments bleibt zu zeigen, dass aus $L = K(\alpha, \beta)$ folgt, $L = K(\gamma)$ für irgendein $\gamma \in L$.

Sein $\mathfrak{m}_\alpha$ und $\mathfrak{m}_\beta$ die zugehörigen Minimalpolynome. Bei Definition haben wir $\mathfrak{m}_\alpha(\alpha) = 0$. Sein $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n \in L$ alle Nullstellen des Minimalpolynoms $\mathfrak{m}_\alpha$. Gleichwie, sein $\beta = \beta_1, \beta_2, \ldots, \beta_m \in L$ die Nullstellen von $\mathfrak{m}_\beta$.
Behauptung 1: Es gibt ein $c \in K$, so dass für alle $i \neq j$, $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, m\}$,

$$\alpha + c\beta \neq \alpha_i + c\beta_j.$$

Dies ist möglich, da für jeden i, j, die Funktion $\alpha + x\beta - \alpha_i - x\beta_j = 0$ nur endliche viele (eigentlich maximal eine) Lösung haben kann und K unendlich viele Elemente hat (da es einen Ringhomomorphismus von K nach $\mathbb{C}$ gibt und daher K Charakteristik null hat).

Sei $\gamma = \alpha + c\beta$, wo c wie in der Behauptung ist. Es bleibt zu zeigen, dass $K(\gamma) = K(\alpha, \beta)$. Da $\gamma = \alpha + c\beta \Rightarrow K(\gamma) \subseteq K(\alpha, \beta)$. Für die andere Seite bleibt zu zeigen, dass $\alpha, \beta \in K(\gamma)$. Definiere dazu

$$r(x) := \mathfrak{m}_\alpha(\gamma - cx) = (\gamma - cx) \circ \mathfrak{m}_\alpha(x).$$

Behauptung 2: Die einzige gemeinsame Nullstelle von $r(x)$ und $\mathfrak{m}_\beta(x)$ ist β.

Es gilt $r(\beta) = \mathfrak{m}_\alpha(\alpha) = 0$. Daher ist β eine gemeinsame Nullstelle von $r(x)$ und $\mathfrak{m}_\beta$. Da c so gewählt war, dass $\alpha + c\beta - c\beta_j \neq \alpha_i$, es sei denn $i = j = 1$ und $\{\alpha = \alpha_1, \ldots, \alpha_n\}$ die einzigen Nullstellen von $\mathfrak{m}_\alpha$ sind, gilt $r(\beta_j) \neq 0$ für alle $j \neq 1$. Weil aber $\{\beta = \beta_1, \ldots, \beta_m\}$ die einzigen Nullstellen von $\mathfrak{m}_\beta$ sind, folgt die Behauptung.

Sei $\mathfrak{n}_\beta$ das Minimalpolynom von β, aber über $K(\gamma)$. Korollar 1.3.8 impliziert, dass $\mathfrak{n}_\beta | \mathfrak{m}_\beta$ und $\mathfrak{n}_\beta | r$, da $\mathfrak{m}_\beta(\beta) = 0$ und $r(\beta) = 0$, wobei $\mathfrak{m}_\beta$ und r nun als Polynome über $K(\gamma)$ aufgefasst werden.

Daher ist jede Nullstelle von $\mathfrak{n}_\beta$ eine gemeinsame Nullstelle von $\mathfrak{m}_\beta$ und r. Behauptung 2 sagt nun, dass die einzige Nullstelle von $\mathfrak{n}_\beta$, β ist.

Galois Separabelitätssatz 2.1.2 sagt nun, dass $\mathfrak{n}_\beta = x - \beta$ sein muss, daher, $\beta \in K[\gamma]$. Da $\beta \in K(\gamma)$, folgt, dass $c\beta \in K(\gamma)$, da $c \in K$. Daher ist $\gamma - c\beta = \alpha \in K(\gamma)$ und der Satz ist bewiesen. □

Beispiel 2.1.5. Wir wollen zeigen, dass das Element $\alpha = \sqrt{2} + \sqrt{3}$ primitiv ist in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Wir erinnern uns dazu an Beispiel 1.3.34, wo wir gezeigt haben, dass das Minimalpolynom von $\sqrt{2}+\sqrt{3}$ $\mathfrak{m}_\alpha = x^4 - 10x^2 + 1$ ist. Daher ist $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$, laut Lemma 1.3.28.

Auf der anderen Seite ist $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ und der Körperturmsatz 1.3.30 besagt, dass $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \leq 4$. Da $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, müssen sie isomorph sein.

Wir fassen unsere Diskussion zusammen:

Bemerkung 2.1.6. Laut dem Satz vom primitiven Element ist jeder algebraische Zahlenkörper von der Form $\mathbb{Q}(\alpha)$, wo $\alpha \in \hat{\mathbb{Q}} = \mathbb{C}_{\mathbb{Q}}^{\mathsf{alg}}$ eine algebraische Zahl ist. Der Grad der Erweiterung ist der Grad des Minimalpolynoms $\mathfrak{m}_\alpha$ von α.

Lemma 2.1.7. *Sei K ein algebraisches Zahlenkörper und $\sigma : K \to \mathbb{C}$ ein Ringhomomorphismus. Es gilt $\sigma(x) = x$ für jeden $x \in \mathbb{Q}$.*

Zur Erläuterung, wir identifizieren $x = \frac{a}{b} \in \mathbb{Q}$ mit $x \in K$ (bzw. $x \in \mathbb{C}$), da es genau einen Ringhomomorphismus $\mathbb{Q} \to K$ (bzw. $\mathbb{Q} \to \mathbb{C}$) gibt (Proposition 1.2.20).

Beweis. Bei Definition eines algebraischen Zahlenkörpers gibt es einen Ringhomomorphismus $f : \mathbb{Q} \to K$. Daher ist $\sigma \circ f$ ein Ringhomomorphismus von $\mathbb{Q}$ nach $\mathbb{C}$. Da es laut Proposition 1.2.20 nur einen solchen Homomorphismus gibt, muss es die wohlbekannte Einbettung $\mathbb{Q} \to \mathbb{C}$, $\frac{a}{b} \mapsto \frac{a}{b} + 0i$ sein. □

Lemma 2.1.8. *Sei $f \in \mathbb{Q}[X]$ und $\sigma : K \to \mathbb{C}$ eine Einbettung. Es gilt*

$$f(\sigma(x)) = \sigma(f(x)),$$

für alle $x \in K$.

Beweis. Sei $f(x) = \sum a_n x^n$, mit $a_i \in \mathbb{Q}$. Da σ ein Ringhomomorphismus ist (und daher mit + und × verträglich), folgt:

$$\begin{aligned} \sigma(f(x)) &= \sigma\left(\sum a_n x^n\right) \\ &= \sum \sigma(a_n)\sigma(x)^n \\ &= \sum a_n \sigma(x)^n \\ &= f(\sigma(x)) \end{aligned}$$

Die vorletzte Gleichung ist Lemma 2.1.7. □

Korollar 2.1.9. *Sei $K = \mathbb{Q}(\alpha)$, α algebraisch und $\sigma : K \to \mathbb{C}$ eine Einbettung. Dann ist σ eindeutig durch $\sigma(\alpha)$ festgelegt.*

Beweis. Sei $r \in K$. Da α algebraisch ist, ist jedes Element von K algebraisch über $\mathbb{Q}$. Daher, $r = g(\alpha)$, für irgendein $g \in \mathbb{Q}[X]$. Lemma 2.1.8 besagt nun, dass $\sigma(r) = g(\sigma(\alpha)) = \sigma(g(\alpha))$. Daher ist es durch α polynomial festgelegt. □

Definition 2.1.10. Zwei algebraische Zahlen heißen *K-konjugiert* wenn sie das selbe Minimalpolynom über K haben.

Wir werden nur den Fall $K = \mathbb{Q}$ brauchen. Anstatt $\mathbb{Q}$-konjugiert werden wir einfach nur konjugiert sagen.

Lemma 2.1.11. *Sei $\sigma : K \to \mathbb{C}$ eine Einbettung. Die Elemente $\alpha \in K$ und $\sigma(\alpha) \in \mathbb{C}$ sind konjugiert.*

Beweis. Es gilt $\mathfrak{m}_\alpha(\sigma(\alpha)) = \sigma(\mathfrak{m}_\alpha(\alpha)) = \sigma(0) = 0$, wobei die erste Gleichung Lemma 2.1.8 ist. □

Satz 2.1.12. *Sei $[K : \mathbb{Q}] = d$. Es gibt genau d Einbettungen $K \to \mathbb{C}$.*

Beweis. Sein $K = \mathbb{Q}(\alpha)$, $\mathfrak{m}_\alpha$ das Minimalpolynom von α und $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ die Konjugierten von α.

- Eine Einbettung $\sigma : K \to \mathbb{C}$ wird eindeutig durch $\sigma(\alpha)$ festgelegt (Korollar 2.1.9);
- Beim Ringhomomorphismus muss jede polynomiale Gleichung, dass von $\alpha \in K$ erfüllt wird, auch von $\sigma(\alpha) \in \mathbb{C}$ erfüllt werden: Aus $\mathfrak{m}_\alpha(\alpha) = 0 \Rightarrow \mathfrak{m}_\alpha(\sigma(\alpha)) = 0$.

Es folgt, dass bei einer Einbettung $\sigma : K \to \mathbb{C}$, α auf einen der $\sigma(\alpha_i)$'s abbilden muss. Daher gibt es maximal d Einbettungen $K \to \mathbb{C}$. Zu sehen, dass es wirklich d verschiedene gibt, erinnern wir uns an dem Körperisomorphismus

$$\mathbb{Q}(\alpha) \to \mathbb{Q}[X]/(\mathfrak{m}_\alpha), \quad \alpha \mapsto \overline{x}.$$

Da $\mathfrak{m}_\alpha(\alpha_i) = 0$ für jeden Konjugierten $\alpha_i \in \mathbb{C}$ von α, folgt, dass die Abbildung

$$\mathbb{Q}[X]/(\mathfrak{m}_{\alpha_i}) \to \mathbb{C} \quad \overline{f(x)} \mapsto f(\alpha_i)$$

auch wirklich ein Ringhomomorphismus definiert. □

Beispiel 2.1.13. Sei $K = \mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Die 2 Einbettungen $\sigma_i : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}, i = 1, 2$ sind

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}, \quad \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}.$$

Beispiel 2.1.14. Sei $K = \mathbb{Q}(\alpha)$, wobei $\mathfrak{m}_\alpha = x^3 + 2x + 2$. Dies ist irreduzibel laut Eisensteins Kriterium. Wir haben $[K : \mathbb{Q}] = 3$ und

$$K = \mathbb{Q}(\alpha) := \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}.$$

Sein β, γ die zwei weiteren Nullstellen von $\mathfrak{m}_\alpha$ über $\mathbb{C}$. Die drei Einbettungen sind

$$\sigma_1(a + b\alpha + c\alpha^2) = a + b\alpha + c\alpha^2, \quad \sigma_2(a + b\alpha + c\alpha^2) = a + b\beta + c\beta^2 \text{ und } \sigma_3(a + b\alpha + c\alpha^2) = a + b\gamma + c\gamma^2.$$

2.2 Die Norm, die Spur und die Diskriminante

Definition 2.2.1. Sei K eine algebraische Körpererweiterung von $\mathbb{Q}$ mit Grad d und $\sigma_1, \ldots, \sigma_d$ die Einbettungen von K in $\mathbb{C}$. Für $k \in K$ definieren wir die *Norm* und die *Spur* wie folgt:

$$\mathsf{N}(k) \coloneqq \prod_{i=1}^{d} \sigma_i(k) \quad \text{und} \quad \mathsf{Sp}(k) \coloneqq \sum_{i=1}^{d} \sigma_i(k).$$

Lemma 2.2.2. *Sei K ein algebraisches Zahlenkörper und $x \in K$. Sei $x_i = \sigma_i(x)$ ein Konjugiertes von x. Dann ist*

$$\mathsf{N}(x) = \mathsf{N}(x_i)$$

und

$$\mathsf{Sp}(x) = \mathsf{Sp}(x_i).$$

Beweis. Dies folgt von den Definitionen, da wir das Produkt, bzw. die Summe, über alle Konjugierten nehmen. □

A priori sind von der Definition die Norm und die Spur nur komplexe Zahlen. Es gilt aber:

Proposition 2.2.3. *Sei K eine endliche Körpererweiterung von $\mathbb{Q}$. Für jeden $k \in K$ gilt $\mathsf{N}(k) \in \mathbb{Q}$ und $\mathsf{Sp}(k) \in \mathbb{Q}$.*

Beweis. Sei $K = \mathbb{Q}(\alpha)$ und $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ alle Konjugierten von α. Wir haben $k = g(\alpha)$ für irgendein $g \in \mathbb{Q}[X]$. Daher gilt

$$\mathsf{N}(k) = \prod_{i=1}^{n} \sigma_i(g(\alpha)) = \prod_{i=1}^{n} g(\sigma_i(\alpha)) = \prod_{i=1}^{n} g(\alpha_i)$$

und

$$\mathsf{Sp}(k) = \sum_{i=1}^{n} \sigma_i(g(\alpha)) = \sum_{i=1}^{n} g(\sigma_i(\alpha)) = \sum_{i=1}^{n} g(\alpha_i).$$

Die jeweils letzte Gleichung gilt nach einer Neuordnung. Da $S(x_1, \cdots, x_n) \coloneqq \prod_{i=1}^{n} g(x_i)$ und $S'(x_1, \cdots, x_n) \coloneqq \sum_{i=1}^{n} g(x_i)$ klar symmetrisch mit Bezug zu $\alpha_1, \alpha_2, \ldots, \alpha_n$ sind, können wir Korollar 1.5.19, mit $f = \mathfrak{m}_\alpha$, benutzen und erhalten so die Aussage. □

Bemerkung 2.2.4. Man sollte auch erwähnen, dass nicht jedes der $\sigma_i(g(\alpha))$ in K liegen müssen. Wenn alle in K sind, heißt so eine Erweiterung Galois'sch. Sieh Bemerkung 2.2.17.

Proposition 2.2.5. *Es gilt $\mathsf{N}(k) = 0$ genau dann wenn $k = 0$.*

Beweis. Bei Definition ist die Norm von k genau dann Null, wenn es eine Einbettung $\sigma_i : K \to \mathbb{C}$ gibt, mit $\sigma_i(k) = 0$. Da aber jede Abbildung zwischen Körpern injektiv ist (Proposition 1.1.52), passiert dies genau dann wenn $k = 0$ ist. □

Proposition 2.2.6. *Es gilt:*

$$\mathsf{N}(xy) = \mathsf{N}(x)\mathsf{N}(y)$$

und

$$\mathsf{Sp}(x + y) = \mathsf{Sp}(x) + \mathsf{Sp}(y).$$

Beweis. Folgt fast von der Definition. Wir haben

$$\mathsf{N}(xy) = \prod_{i=1}^{n} \sigma_i(xy) = \prod_{i=1}^{n} \sigma_i(x) \prod_{i=1}^{n} \sigma_i(y) = \mathsf{N}(x)\mathsf{N}(y)$$

und

$$\mathsf{Sp}(xy) = \sum_{i=1}^{n} \sigma_i(x + y) = \sum_{i=1}^{n} \sigma_i(x) + \sum_{i=1}^{n} \sigma_i(y) = \mathsf{N}(x) + \mathsf{N}(y).$$

□

Beispiel 2.2.7. Sei $K = \mathbb{Q}(\sqrt{2})$. Es gilt

$$\mathsf{N}(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$$

und

$$\mathsf{Sp}(a + b\sqrt{2}) = (a + b\sqrt{2}) + (a - b\sqrt{2}) = 2a.$$

Lemma 2.2.8. *Sei $K = \mathbb{Q}(\alpha)$ mit $[K : \mathbb{Q}] = d$ und $r \in \mathbb{Q}$. Dann ist*

$$\mathsf{N}(r) = r^d \qquad \text{und} \qquad \mathsf{Sp}(r) = dr.$$

Beweis. Laut Lemma 2.1.7 ist $\sigma_i(r) = r$ für jeden $r \in \mathbb{Q}$. Das Lemma folgt nun von der Definition der Norm und der Spur. □

Lemma 2.2.9. *Sei $K = \mathbb{Q}(\alpha)$ und $r \in \mathbb{Q}$. Dann gilt*

$$\mathsf{N}(r - \alpha) = \mathfrak{m}_\alpha(r).$$

Beweis. Dies folgt von den Definitionen. Sein $\{\alpha = \alpha_1, \ldots, \alpha_d\}$ die Konjugierten von α. Also,

$$\mathfrak{m}_\alpha(x) = (x - \alpha_1)\cdots(x - \alpha_d)$$

über $\mathbb{C}$. Bei Definition der Norm haben wir

$$\mathsf{N}(r - \alpha) = (r - \alpha_1)\cdots(r - \alpha_d),$$

was freilich die Auswertung von $\mathfrak{m}_\alpha$ auf $x = r \in \mathbb{Q}$ ist. □

Korollar 2.2.10. *Sei $K = \mathbb{Q}(\alpha)$ und a_0 das freie Term des Minimalpolynoms $\mathfrak{m}_\alpha$ von α. Dann gilt*

$$\mathsf{N}(\alpha) = (-1)^d a_0,$$

wobei $d = \mathsf{grad}(\mathfrak{m}_\alpha)$.

Beweis. Die Multiplikativität der (Proposition 2.2.6) Lemma 2.2.9, angewandt auf $r = 0$ besagt

$$\mathsf{N}(\alpha) = \mathsf{N}(-1)\mathsf{N}(-\alpha) = (-1)^d \mathfrak{m}_\alpha(0) = (-1)^d a_0,$$

wobei $\mathsf{N}(-1) = (-1)^d$ laut Lemma 2.2.8. □

Definition 2.2.11. Sei $\mathcal{B} = \{b_1, \ldots, b_d\}$ eine Basis von K als $\mathbb{Q}$-Vektorraum. Wir definieren die *Diskriminante*, gezeichnet $\Delta(\mathcal{B})$, als

$$\Delta(\mathcal{B}) = \det(\mathsf{Sp}(b_i b_j)_{i,j=1}^d).$$

Das heißt, wir nehmen die Determinante der Matrix, dessen ij-es Eintrag $\mathsf{Sp}(b_i b_j)$ ist. Da laut Proposition 2.2.3 $\mathsf{Sp}(x)$ immer in $\mathbb{Q}$ ist, ist die Diskriminante immer eine rationale Zahl.

Proposition 2.2.12. *Sei K eine algebraische Körpererweiterung von $\mathbb{Q}$, $\sigma_1, \ldots, \sigma_d : K \to \mathbb{C}$ die Körpereinbettungen von K und $\mathcal{B} = \{b_1, \ldots, b_d\}$ eine Basis von K als $\mathbb{Q}$-Vektorraum. Es gilt*

$$\Delta(\mathcal{B}) = \det(\sigma_i(b_j))^2.$$

Bemerkung 2.2.13. Hier ist die Determinante der Matrix gemeint, dessen ij-er Eintrag $\sigma_i(b_j)$ ist. Das ganze wird dann nochmal quadriert. Dies heißt jedoch *nicht*, dass die Diskriminante immer positiv ist, da $\det(\sigma_i(b_j))$ ja keine reelle Zahl sein muss. Von Definition 2.2.11 wissen wir nur, das dessen Quadrat rational ist.

Bemerkung 2.2.14. Die Determinante macht Sinn, da die Matrix laut Satz 2.1.12 quadratisch ist.

Beweis. [Beweis von Proposition 2.2.12] Sei $A = (\sigma_i(b_j))$. Der ij-te Eintrag von A^tA ist gegeben durch

$$(A^tA)_{ij} = \sum_k \sigma_k(b_i)\sigma_k(b_j) = \sum_k \sigma_k(b_ib_j) = \mathsf{Sp}(b_ib_j)$$

bei Definition der Spur. Die vorletzte Gleichung gilt, da σ ein Ringhomomorphismus ist und sich daher mit der Addition wohl verträgt. □

Beispiel 2.2.15. Sei $K = \mathbb{Q}(\sqrt{2})$ und $\mathcal{B} = \{1, \sqrt{2}\}$. Wir haben

$$\Delta(\mathcal{B}) = \left(\det\begin{bmatrix}1 & \sqrt{2}\\ 1 & -\sqrt{2}\end{bmatrix}\right)^2 = 8.$$

Beispiel 2.2.16. Sei $K = \mathbb{Q}(\sqrt[3]{2})$ und $\mathcal{B} = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. Bezeichne mit $1 \neq \zeta_3 \in \mathbb{C}$ eines der nichttrivialen kubischen Wurzeln der 1. Z.B., sei $\zeta_3 := -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Wir hätten auch dessen Quadrat, nämlich $-\frac{1}{2} - i\frac{\sqrt{3}}{2}$ nähmen können. Wir haben

$$\Delta(\mathcal{B}) = \left(\det\begin{bmatrix}1 & \sqrt[3]{2} & \sqrt[3]{4}\\ 1 & \sqrt[3]{2}\zeta_3 & \sqrt[3]{4}\zeta_3^2\\ 1 & \sqrt[3]{2}\zeta_3^2 & \sqrt[3]{4}\zeta_3\end{bmatrix}\right)^2 = 4 \times 27 = 108.$$

Hier bedenke man, dass $(\zeta_3^2)^2 = \zeta_3$ ist.

Bemerkung 2.2.17. Eine kleine Erinnerung an Galois Theorie besagt, dass die Konjugierten α_i von α im Allgemeinen nicht in $\mathbb{Q}(\alpha)$ sind. Die liegen alle genau dann in $\mathbb{Q}(\alpha)$, wenn die Körpererweiterung zusätzlich Galois, bzw. normal ist. Z.B., $\mathbb{Q}(\sqrt[3]{2})$ is nicht Galois da $\zeta_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ nicht reell ist, daher kann es nicht in $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ liegen. Jedoch wäre $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ eine Galois Erweiterung. Der Grad dieser Erweiterung wäre jedoch 6, nicht 3.

Wie schon aus Lineare Algebra I & II bekannt, gibt es im allgemeinen viele Basen für einen Vektorraum. Die Diskriminante ist *nicht* invariant unter Basiswechsel, jedoch gibt es eine einfache Formel.

Korollar 2.2.18. *Sei K eine algebraische Körpererweiterung von $\mathbb{Q}$ und $\mathcal{B} = \{b_1 \ldots, b_d\}, \mathcal{C} = \{c_1, \ldots, c_d\}$ zwei Basen von K als $\mathbb{Q}$-Vektorraume. Sei $M_{\mathcal{C}}^{\mathcal{B}}$ der Übergangsmatrix von $\mathcal{B}$ nach $\mathcal{C}$ (i.e., $c_i = \sum \lambda_{i,j} b_j$). Es gilt*

$$\Delta(\mathcal{C}) = \det(M_{\mathcal{C}}^{\mathcal{B}})^2 \Delta(\mathcal{B}).$$

Bemerkung 2.2.19. Da eine Übergangsmatrix invertierbar ist und die Determinante einer invertierbaren Matrix eine Einheit des Basisringes (in unserem Fall des Körpers $\mathbb{Q}$) ist, ist die Diskriminante einer Basis eindeutig bis auf einer Einheit. Zur Erinnerung, in der Algebra ist dies "nahe genug", sogar die Faktorisierung in der ganzen Zahlen in Primzahlen ist nur bis zur Einheit eindeutig: $2 \cdot 5 = (-1) \cdot 2 \cdot (-1) \cdot 5$.

2.2.1 Die Standardbasis

Vandermondes Determinante

Lemma 2.2.20. *Sei $K = \mathbb{Q}(\alpha)$ mit $[K : \mathbb{Q}] = d$. Dann ist*

$$\mathcal{A} = \{1, \alpha, \ldots, \alpha^{d-1}\}$$

eine Basis von K als $\mathbb{Q}$-Vektorraum.

Beweis. Dies ist quasi Aufgabe 30 unter Bezug von Bemerkung 2.1.6. □

Da wir für jede algebraische Körpererweiterung K von $\mathbb{Q}$ einen Elementen $\alpha \in \mathbb{C}$, mit $K = \mathbb{Q}(\alpha)$, finden können (Satz vom primitiven Element 2.1.4), können wir immer so eine Basis konstruieren. Für solch eine Basis ist es relativ einfach die Diskriminante auszurechnen, wie man es an der folgenden Formel sieht:

Satz 2.2.21 (Vandermondes). *Sei R ein Ring, $X_1, \dots, X_d \in R$ Elemente des Ringes und bezeichne*

$$\mathcal{M}_X := \begin{bmatrix} 1 & X_1 & \cdots & X_1^{d-1} \\ 1 & X_2 & \cdots & X_2^{d-1} \\ \vdots & & \vdots & \vdots \\ 1 & X_d & \cdots & X_d^{d-1} \end{bmatrix}.$$

Es gilt

$$\det(\mathcal{M}_X) = \prod_{i<j} (X_j - X_i).$$

Beweis. Wir werden es durch Induktion auf d beweisen. Bei $d = 2$ is es klar und wir nehmen es für $d-1$ an. Um den Induktionsschritt zu beweisen, betrachten wir die Determinante von $\mathcal{M}_X$ als eine Funktion in der Variable X_d. (Die Variablen $X_1, \dots, X_{d-1}$ sehen wir als Konstant an). Es ist klar, dass $\det(\mathcal{M}_X)$ ein Polynom von Grad $d-1$ ist.

Ein jedes Polynom $f(x)$ vom Grad n, mit Wurzeln $z_1, \dots, z_n$ kann man als

$$f(x) = c(x - z_1)(x - z_2)\cdots(x - z_n)$$

schreiben, wobei c das Leitkoeffizient ist.

In unserem Fall ist das Leitkoeffizient von $\det(\mathcal{M}_X)$ die Determinante

$$c = \det \begin{bmatrix} 1 & X_1 & \cdots & X_1^{d-2} \\ 1 & X_2 & \cdots & X_2^{d-2} \\ \vdots & & \vdots & \vdots \\ 1 & X_{d-1} & \cdots & X_{d-1}^{d-2} \end{bmatrix},$$

welches, nach Induktionsannahme, gleich $\prod_{1 \le i < j \le d-1} (X_j - X_i)$ ist. Die Wurzeln sind $X_1, \dots, X_{d-1}$: Um sich davon zu überzeugen, setze $X_d = X_i, i \le d-1$. Dann werden sich zwei Zeilen wiederholen und als solches wird die Determinante gleich null werden. (Lineare Algebra). Es gilt daher

$$\det(\mathcal{M}_X) = \left[\prod_{1 \le i < j \le d-1} (X_j - X_i) \right] \times [(X_d - X_1)(X_d - X_2)\cdots(X_d - X_{d-1})] = \prod_{i<j} (X_j - X_i).$$

□

Beweis. [Alternativer/direkter Beweis von Satz 2.2.21] Wir werden es durch Induktion auf d beweisen. Es ist klar bei $d = 2$. Wir nehmen an, dass es für $d-1$ hält. Wir haben

$$\det \begin{bmatrix} 1 & X_1 & \cdots & X_1^{d-1} \\ 1 & X_2 & \cdots & X_2^{d-1} \\ \vdots & & \vdots & \vdots \\ 1 & X_d & \cdots & X_d^{d-1} \end{bmatrix} = \det \begin{bmatrix} 0 & X_1 - X_d & \cdots & X_1^{d-1} - X_d^{d-1} \\ 0 & X_2 - X_d & \cdots & X_2^{d-1} - X_d^{d-1} \\ \vdots & & \vdots & \vdots \\ 1 & X_d & \cdots & X_d^{d-1} \end{bmatrix} = (-1)^{d-1} \det \begin{bmatrix} X_1 - X_d & \cdots & X_1^{d-1} - X_d^{d-1} \\ X_2 - X_d & \cdots & X_2^{d-1} - X_d^{d-1} \\ \vdots & & \vdots \\ X_{d-1} - X_d & \cdots & X_{d-1}^{d-1} - X_d^{d-1} \end{bmatrix}.$$

Man erinnere sich, dass $X^n - Y^n = (X - Y)(X^{n-1} + X^{n-2}Y + \cdots + XY^{n-2} + Y^{n-1})$. Daher können wir das ganze weiter vereinfachen als

$$= (-1)^{d-1} \prod_{i=1}^{d-1} (X_i - X_d) \det \begin{bmatrix} 1 & X_1 + X_d & \cdots & X_1^{d-2} + \cdots + X_d^{d-2} \\ 1 & X_2 + X_d & \cdots & X_2^{d-2} + \cdots + X_d^{d-2} \\ \vdots & & \vdots & \vdots \\ 1 & X_{d-1} + X_d & \cdots & X_{d-1}^{d-2} + \cdots + X_d^{d-2} \end{bmatrix} = \prod_{i=1}^{d-1} (X_d - X_i) \det \begin{bmatrix} 1 & X_1 & \cdots & X_1^{d-2} \\ 1 & X_2 & \cdots & X_2^{d-2} \\ \vdots & & \vdots & \vdots \\ 1 & X_{d-1} & \cdots & X_{d-1}^{d-2} \end{bmatrix}.$$

Für die letzte Gleichung multiplizieren wir die erste Spalte (die mit den ganzen 1-en) mit X_d und ziehen es von der zweiten Spalte ab. Dann multiplizieren wir die ersten beiden Spalten mit X_d und ziehen beide von der dritten Spatel ab usw. Dadurch ändert sich die Determinante ja bekanntlich nicht. Unsere Induktionsannahme gibt uns nun

$$= \prod_{i=1}^{d-1} (X_d - X_i) \prod_{1 \le i < j \le d-1} (X_j - X_i) = \prod_{1 \le i < j \le d} (X_j - X_i) = \prod_{i<j} (X_j - X_i)$$

□

Korollar 2.2.22. *Sei $\alpha \in \mathbb{C}$ algebraisch über $\mathbb{Q}$ und $\alpha = \alpha_1, \ldots, \alpha_d$ die Konjugierten von α. Dann ist $\mathcal{A} := \{1, \alpha, \ldots, \alpha^{d-1}\}$ eine Basis von $\mathbb{Q}(\alpha)$ und es gilt*

$$\Delta(\mathcal{A}) = \prod_{i<j} (\alpha_j - \alpha_i)^2.$$

Beweis. Dies ist eine Zusammensetzung von Lemma 2.2.20, Proposition 2.2.12 und Satz 2.2.21. □

Korollar 2.2.23. *Sei K algebraisch über $\mathbb{Q}$. Für jede Basis $\mathcal{B}$ von K als $\mathbb{Q}$-Vektorraum gilt $\Delta(\mathcal{B}) \neq 0$.*

Beweis. Dies folgt von Satz 2.1.4 und Korollaren 2.2.18 und 2.2.22. Ausführlicher: Da K algebraisch ist, gibt es ein $\alpha \in \mathbb{C}$, so dass $K = \mathbb{Q}(\alpha)$, laut Satz 2.1.4. Für die Basis $\mathcal{A} = \{1, \alpha, \ldots, \alpha^{d-1}\}$ gilt, dass $\Delta(\mathcal{A}) \neq 0$, wie in Korollar 2.2.22 gezeigt. Da die Determinante einer jeden Basiswechselmatrix ungleich null ist (Lineare Algebra), impliziert Korollar 2.2.18 nun unsere Aussage. □

Diskriminante der Standardbasis von $\mathbb{Q}(\alpha)$

Satz 2.2.24. *Sei $K = \mathbb{Q}(\alpha)$ mit $[K : \mathbb{Q}] = d$, $\mathfrak{m}'_\alpha$ die Ableitung das Minimalpolynom von α und $\mathcal{A} = \{1, \alpha, \ldots, \alpha^{d-1}\}$. Wir haben*

$$\Delta(\mathcal{A}) = (-1)^{\frac{d(d-1)}{2}} \mathsf{N}(\mathfrak{m}'_\alpha(\alpha)).$$

Beweis. Sein $\alpha = \alpha_1, \cdots, \alpha_d \in \mathbb{C}$ die Konjugierten von α, also die Nullstellen von $\mathfrak{m}_\alpha$. Korollar 2.2.22 ergibt direkt

$$\Delta(\mathcal{A}) = \prod_{i<j} (\alpha_j - \alpha_i)^2 = (-1)^{\frac{d(d-1)}{2}} \prod_{i \neq j} (\alpha_j - \alpha_i).$$

Es bleibt also zu zeigen, dass $\mathsf{N}(\mathfrak{m}'_\alpha(\alpha)) = \prod_{i \neq j} (\alpha_j - \alpha_i)$. Da die α_i's alle Nullstellen von $\mathfrak{m}_\alpha$ über $\mathbb{C}$ sind, haben wir die Zerlegung

$$\mathfrak{m}_\alpha = \prod_{i=1}^{d} (x - \alpha_i),$$

was nach Leibniz

$$\mathfrak{m}'_\alpha = \sum_{k=1}^{d} \prod_{i \neq k} (x - \alpha_i)$$

ergibt. Zur Erläuterung, die Summanden sind Produkte der Form $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_d)$, wobei jeweils eines der α_k's fehlt. Wenn wir $x = \alpha_i$ einsetzen, wird jedes der Summanden Null werden, außer den, der $(x - \alpha_i)$ nicht enthält. Dies ergibt

$$\mathfrak{m}'_\alpha(\alpha_i) = \prod_{j \mid i \neq j} (\alpha_j - \alpha_i). \tag{9}$$

Mit $j \mid i \neq j$ meinen wir, dass wir das Produkt über j nehmen, aber den einen Fall $j = i$ auslassen. Im Vergleich, wenn nur $i \neq j$ unter dem Produkt hätten, würde sowohl i, wie auch j, alle Möglichkeiten durchlaufen, außer $i = j$.

Wir kehren zurück zur Norm: Wir haben

$$\mathsf{N}(\mathfrak{m}'_\alpha(\alpha)) = \prod_i (\mathfrak{m}'_\alpha(\alpha_i)),$$

da die Konjugierten von $f(\alpha)$ natürlich $f(\alpha_i)$ sind. Man setze Formel (9) ein und erhalte

$$\mathsf{N}(\mathfrak{m}'\alpha(\alpha)) = \prod_{i \neq j} (\alpha_j - \alpha_i).$$

□

Korollar 2.2.25. *Sei $K = \mathbb{Q}(\alpha)$ mit $[K : \mathbb{Q}] = d$ und $\beta = \alpha + r$, $r \in \mathbb{Q}$. Dann gilt*

$$\Delta(1, \alpha, \ldots, \alpha^{d-1}) = \Delta(1, \beta, \ldots, \beta^{d-1}).$$

Beweis. Sei $\mathfrak{m}_\alpha$ das Minimalpolynom von α. Dann ist

$$\mathfrak{m}_\beta(x) = \mathfrak{m}_\alpha(x - r)$$

das Minimalpolynom von β, also gilt auch

$$\mathfrak{m}'_\beta(x) = \mathfrak{m}'_\alpha(x - r),$$

woraus direkt

$$\mathfrak{m}'_\beta(\beta) = \mathfrak{m}'_\alpha(\beta - r) = \mathfrak{m}'_\alpha(\alpha + r - r) = \mathfrak{m}'_\alpha(\alpha)$$

folgt. Satz 2.2.24 sagt nun

$$\begin{aligned} \Delta(1, \beta, \ldots, \beta^{d-1}) &= (-1)^{\frac{d(d-1)}{N2}} \mathsf{N}(\mathfrak{m}'_\beta(\beta)) \\ &= (-1)^{\frac{d(d-1)}{N2}} \mathsf{N}(\mathfrak{m}'_\alpha(\alpha)) \\ &= \Delta(1, \alpha, \ldots, \alpha^{d-1}). \end{aligned}$$

□

Bemerkung 2.2.26. Aufgepasst, hier nehmen wir die Potenzen von β genommen, nicht

$$\{1, \alpha + r, \alpha^2 + r, \ldots, \alpha^{d-1} + r\}$$

etc.

Aufgaben

Aufgaben 6

Aufgabe 39 (1 Punkt). Sei K ein algebraisches Zahlenkörper mit

$$[K : \mathbb{Q}] = 2.$$

Beweise, dass $K = \mathbb{Q}(\sqrt{a})$, für irgendeine quadratfreie Zahl $a \in \mathbb{Z}$.

Aufgabe 40 (1 Punkt). Sein $\alpha, \beta \in \mathbb{C}$, so dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = 2$. Beweise, dass

$$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + \beta).$$

Aufgabe 41 (5 Punkte). Sei $K = \mathbb{Q}(\alpha)$, wobei $\alpha = \sqrt{2} + \sqrt{3}$.

i) Finde die Konjugierten von α.

ii) Liste alle Einbettungen $K \to \mathbb{C}$.

iii) Finde die Norm und die Spur von α.

iv) Zeige, dass

$$\mathcal{B} = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$$

eine $\mathbb{Q}$-Basis von K ist.

v) Berechne die Diskriminante

$$\Delta(\mathcal{B}).$$

Aufgabe 42 (1 Punkt). Sei $[L : K] = p$ eine Primzahl. Beweise, dass jedes Element $\alpha \in L \setminus K$ primitiv ist. Das heißt, dass

$$L = K(\alpha).$$

Aufgabe 43 (4 Punkte). Sei $\alpha = \sqrt[3]{2}$ und $\beta = e^{\frac{2\pi i}{3}}\alpha$. Sei $K = \mathbb{Q}(\alpha, \beta)$.

i) Finde die Konjugierten von α mithilfe des Minimalpolynoms von $\sqrt[3]{2}$.

ii) Zeige, dass $\mathbb{Q}(\alpha) \simeq \mathbb{Q}(\beta)$ indem man das Minimalpolynom von α bestimmt.

iii) Zeige, dass $\alpha \notin \mathbb{Q}(\beta)$ und $\beta \notin \mathbb{Q}(\alpha)$.

iv) Beschreibe alle Einbettungen $K \to \mathbb{C}$.

Aufgabe 44 (2 Punkte). Sei $\alpha = \sqrt[3]{2}$ und $K = \mathbb{Q}(\alpha)$.

i) Zeige, dass

$$\mathcal{B} = \{2, \sqrt[3]{2} + 1, \sqrt[3]{4} + 1\}$$

eine $\mathbb{Q}$-Basis von K ist.

ii) Berechne die Diskriminante

$$\Delta(\mathcal{B}).$$

Aufgabe 45 (3 Punkte). Sein $p, q \in \mathbb{Z}$, so dass $f(x) = X^3 + px + q$ irreduzibel über $\mathbb{Z}[X]$ ist und sei $\alpha \in \mathbb{C}$ eine Wurzel von $f(x)$.

i) Beweise, dass $\mathsf{Sp}(1) = 3, \mathsf{Sp}(\alpha) = 0, \mathsf{Sp}(\alpha^2) = -2p$ und $\mathsf{Sp}(\alpha^3) = -3q$.

ii) Was ist $\mathsf{Sp}(\alpha^4)$?

iii) Beweise, dass

$$\Delta(1, \alpha, \alpha^2) = -4p^3 - 27q^2.$$

2.3 Ganzalgebraische Zahlenringe

Sei K eine algebraische Körpererweiterung von $\mathbb{Q}$.

Definition 2.3.1. Ein Element $\alpha \in K$ wird eine *ganzalgebraische Zahl* oder *ganze algebraische Zahl* genant, wenn es ein normiertes Polynom $f \in \mathbb{Z}[X]$ gibt, so dass $f(\alpha) = 0$.

Da $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$ gilt, macht diese Definition Sinn.

Beispiel 2.3.2. Sei $K = \mathbb{Q}(\sqrt{2})$.

- Das Element $\sqrt{2}$ ist eine ganze algebraische Zahl, da dessen Minimalpolynom $\mathfrak{m}_{\sqrt{2}} = x^2 - 2$ ist. Also gibt es so ein Polynom.
- Das Element $\frac{\sqrt{2}}{2}$ ist keine ganze algebraische Zahl: Dessen Minimalpolynom ist $\mathfrak{m}_{\frac{\sqrt{2}}{2}} = x^2 - \frac{1}{2}$.

  Sei $f(x) \in \mathbb{Z}[X]$ ein Polynom, so dass $\frac{\sqrt{2}}{2}$ eine Nullstelle von $f(x)$ ist. Bei Definition des Minimalpolynoms, mithilfe von dem Lemma von Gauß und der Tatsache, dass die Primitivisation von $\mathfrak{m}_\alpha(x)$ das Polynom $2x^2 - 1$ ist, gibt es ein Polynom $g(x) \in \mathbb{Z}[X]$, so dass $f(x) = (2x^2 - 1)g(x)$. Daher kann $f(x)$ nicht normiert sein, da dessen Leitkoeffizient durch zwei teilbar sein wird.

Proposition 2.3.3. *Sei K eine algebraische Körpererweiterung von $\mathbb{Q}$. Ein Element $\alpha \in K$ ist genau dann eine ganzalgebraische Zahl, wenn dessen Minimalpolynom $\mathfrak{m}_\alpha$ in $\mathbb{Z}[X]$ liegt.*

Beweis. Sei $\mathfrak{m}_\alpha \in \mathbb{Z}[X]$, es ist klar, dass α ganzalgebraisch ist.

Sei α ganzalgebraisch, $\mathfrak{m}_\alpha$ dessen Minimalpolynom und $f(x) \in \mathbb{Z}[X]$ das normiertes Polynom mit $f(\alpha) = 0$. Es gilt zu beweisen, dass $\mathfrak{m}_\alpha \in \mathbb{Z}[X]$. Dies ist Äquivalent zu sagen, dass $\mathfrak{m}_\alpha = \mathfrak{m}_{\alpha p}$ (Primitivisation), was äquivalent ist zu sagen, dass $\mathfrak{m}_{\alpha p} \in \mathbb{Z}[X]$ normiert ist.

Korollar 1.3.8, zusammen mit Satz 1.4.11, sagt aus, dass es ein Polynom $g(x) \in \mathbb{Q}[X]$ gibt, mit $f(x) = f_p(x) = g_p(x)\mathfrak{m}_{\alpha p}(x)$. Da das Leitkoeffizient des Produkts, das Produkt der Leitkoeffizienten ist, muss $\mathfrak{m}_\alpha$ als Leitkoeffizient ± 1 haben. Bei Definition von primitiv muss es 1 sein. □

Korollar 2.3.4. *Ein Element $\alpha \in K$ ist genau dann ganzalgebraisch, wenn dessen Konjugierte $\sigma(\alpha)$ ganzalgebraisch ist.*

Proposition 2.3.5. *Sei K eine endliche/algebraische Körpererweiterung von $\mathbb{Q}$. Ein Element $\alpha \in K$ ist genau dann ganzalgebraisch, wenn $\mathbb{Z}[\alpha]$ endlich erzeugt ist als eine abelsche Gruppe. Äquivalent, wenn $\mathbb{Z}[\alpha]$ ein endlichdimensionales $\mathbb{Z}$-Modul ist.*

Beweis. Man bemerke zuerst, dass Elemente von $\mathbb{Z}[\beta]$, (nicht zwingend algebraisches β), von der Form $b_0 + b_1\beta + b_2\beta^2 + \cdots$ sind, wobei $b_i \in \mathbb{Z}, i \geq 0$. In anderen Worten, als eine abelsche Gruppe ist $\mathbb{Z}[\beta]$ durch $\{\beta^i \mid i \geq 1\}$, allen Potenzen von β, erzeugt.

Sei das Minimalpolynom $\mathfrak{m}_\alpha$ von α vom Grad n. Das heißt

$$\mathfrak{m}_\alpha(x) = x^n + a_{n-1}x^{n-1} \cdots + a_1 x + a_0,$$

wobei $a_i \in \mathbb{Z}$, für alle $0 \leq i \leq n-1$. Wie schon besprochen, ist $\mathbb{Z}[\alpha]$ durch die Menge $\{\alpha^i \mid i \geq 0\}$ erzeugt. Da jedoch von der Definition des Minimalpolynoms folgt, dass $\mathfrak{m}_\alpha(\alpha) = 0$, wissen wir, dass

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots a_1\alpha_1 + \alpha_0).$$

Daher ist $\mathbb{Z}[\alpha]$ von $\{\alpha^i \mid 0 \leq i \leq n-1\}$ erzeugt, also endlich erzeugt.

Auf der anderen Seite, nehmen wir jetzt an, dass $\mathbb{Z}[\alpha]$ endlich erzeugt als eine abelsche Gruppe ist. Das heißt, es gibt eine endliche Teilmenge $\{e_i \in \mathbb{Z}[\alpha] \mid 0 \leq i \leq m\}$, so dass jedes Element von $\mathbb{Z}[\alpha]$ eine Linearkombination der e_i's ist.

Wie am Anfang des Beweises schon besprochen gilt auch, dass jedes e_i eine Linearkombination der α^j's ist. Man kann nicht annehmen, dass es a-priori eine endliche Menge solcher α^j's gibt.

Jedoch braucht man für jedes gegebene Element nur endlich viele (da unendliche Summen in $\mathbb{Z}[\beta]$ nicht existieren). Da wir nur endlich viele e_i's haben, werden wir nur endlich viele der α^j's brauchen um alle e_i's als Linearkombination dieser α^j's zu schreiben. Das heißt, es gibt eine maximale Potenz die vorkommt, welches wir mit α^N bezeichnen. Es gilt:

$$e_i = \sum_{j=0}^{N} a_{i,j}\alpha^j \quad a_{i,j} \in \mathbb{Z},$$

für jeden $0 \leq i \leq m$. Da die $\{e_i\}$'s ein erzeugendes System bilden, gilt auch

$$\alpha^{N+1} = \sum_{i=0}^{m} b_i e_i,$$

wobei $b_i \in \mathbb{Z}$. Zusammengesetz ergibt es

$$\alpha^{N+1} = \sum_{i=0}^{m} b_i \sum_{j=0}^{N} a_{i,j}\alpha^j.$$

Umordnen und das Distributivgesetz ergibt nun

$$\alpha^{N+1} - \sum_{i=0}^{m}\sum_{j=0}^{N} b_i a_{i,j}\alpha^j = 0.$$

Daher gibt es ein Polynom $f(x) \coloneqq x^{N+1} - \sum_{i=0}^{m}\sum_{j=0}^{N} b_i a_{i,j}x^j$, welches klar normiert ist und $f(\alpha) = 0$. Wir haben gezeigt, dass α ganzalgebraisch ist. □

Bemerkung 2.3.6. Um zu sehen, wo Normiertheit ins Spiel kommt, betrachte $\alpha = \frac{\sqrt{2}}{2}$. Dessen Minimalpolynom ist $\mathfrak{m}_\alpha = x^2 - \frac{1}{2}$ und das dazugehörige primitive Polynom ist $2x^2 - 1$. Wir sehen, dass wir $2\alpha^2 = 1$ als Linearkombination von $1 = \alpha^0$ und α ausdrücken können, aber nicht $\alpha^2 = \frac{1}{2}$, da in $\mathbb{Z}$, 2 nicht invertierbar ist.

Hätten wir $\alpha = \sqrt{2}$ genommen, wäre $\alpha^2 = 2 = 2 \times 1$ gewesen, also eine Linearkombination von $1 = \alpha^0$ und α.

Korollar 2.3.7. *Sei K eine algebraische Erweiterung von $\mathbb{Q}$. Die Menge der ganzalgebraischen Zahlen bilden einen Unterring von K.*

Beweis. Die Tatsache, dass 0 und 1 ganzalgebraisch sind ist klar. Sein α und β ganzalgebraische Zahlen. Laut Proposition 2.3.5 gibt es Elemente $\{e_1, \ldots, e_n\}$ und $\{f_1, \ldots, f_m\}$ die $\mathbb{Z}[\alpha]$ und $\mathbb{Z}[\beta]$ als abelsche Gruppen erzeugen.

Es ist klar, dass jedes Element der Form $\alpha^i\beta^j$ in der abelschen Gruppe liegt, welches von all den möglichen Produkten $\{e_1f_1, e_1f_2 \ldots, e_2f_1, \ldots, e_nf_m\}$ erzeugt wird. Wir bezeichnen diese Gruppe mit $\langle\{e_rf_s\}\rangle_{\mathbb{Z}}$. Daher folgt, dass $\mathbb{Z}[\alpha, \beta] \subseteq \langle\{e_rf_s\}\rangle_{\mathbb{Z}}$ eine Untergruppe ist. Da $\langle\{e_rf_s\}\rangle_{\mathbb{Z}}$ endlich erzeugt ist, sind auch alle dessen Untergruppen endlich erzeugt.

Es folgt, dass $\mathbb{Z}[\gamma] \subseteq \mathbb{Z}[\alpha, \beta] \subseteq \langle\{e_rf_s\}\rangle_{\mathbb{Z}}$ endlich erzeugt ist, für $\gamma = \alpha + \beta$ und $\gamma = \alpha\beta$. Proposition 2.3.5 ergibt nun, dass $\alpha + \beta$ und $\alpha\beta$ ganzalgebraisch sind. □

Definition 2.3.8. Sei K eine algebraische Erweiterung von $\mathbb{Q}$ (also ein Zahlenkörper). Das Ring der ganzalgebraischen Elemente von K wird mit $\mathfrak{o}_K$ bezeichnet. Ringe dieser Art werden *algebraische Zahlenringe* genannt.

In Korollar 2.3.7 haben wir gezeigt, dass $\mathfrak{o}_K \subseteq K$ gilt. Die Beziehung ist allerdings stärker. Um es zu beweisen, brauchen wir erst ein kleines Lemma:

Lemma 2.3.9. *Sei K algebraisch über $\mathbb{Q}$. Für jeden $\alpha \in K$ gibt es einen $N \in \mathbb{N}$, so dass $N\alpha \in \mathfrak{o}_K$.*

Beweis. Sei

$$\mathfrak{m}_\alpha = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + x^n$$

und N ein gemeinsames Vielfaches der $\{b_i\}_{i=0}^{n-1}$'s. Dann kann man direkt sehen, dass

$$g(x) := \frac{a_0}{b_0}N^n + \frac{a_1}{b_1}N^{n-1}x + \cdots + \frac{a_{n-1}}{b_{n-1}}Nx^{n-1} + x^n$$

ein normiertes Polynom über $\mathbb{Z}$ ist, dass von $N\alpha$ annihiliert wird, da

$$g(N\alpha) = N^n f(\alpha) = N^n \cdot 0 = 0$$

gilt. □

Korollar 2.3.10. *Sei $K = \mathbb{Q}(\alpha)$ mit*

$$\mathfrak{m}_\alpha = x^n + u_{n-1}x^{n-1} + \cdots + u_1 x + u_0 \quad u_i \in \mathbb{Q}.$$

Es gibt ein $\beta \in \mathbb{C}$ mit Minimalpolynom

$$\mathfrak{m}_\beta = x^n + v_{n-1}x^{n-1} + \cdots + v_1 x + v_0 \quad v_i \in \mathbb{Z},$$

so dass

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\beta).$$

Des weiteren ist $u_i = 0$ genau dann wenn $v_i = 0$.

Beweis. Dies folgt direkt von Lemma 2.3.9 und wir folgen dessen Notation. Sei $\beta = N\alpha$. Es ist klar, dass $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Das einzige, dass wir noch zu beweisen haben ist, dass das Minimalpolynom $\mathfrak{m}_\beta$ von β gleich $g(x)$ ist. Da aber $g(x)$ normiert ist muss man nur noch beweisen, dass es auch irreduzibel ist. Da aber die Grade der Erweiterungen gleich sind, impliziert Lemma 1.3.27 nun das Resultat. Das $u_i = 0 \Leftrightarrow v_i = 0$ ist auch ohne weiteres klar. □

Proposition 2.3.11. *Sei K eine endliche Erweiterung von $\mathbb{Q}$ und $\mathfrak{o}_K$ das Unterring der ganzalgebraischen Zahlen. Dann gilt*

1. *Das Ring $\mathfrak{o}_K$ ist ein Integritätsbereich;*
2. *Der Quotientenkörper von $\mathfrak{o}_k$ ist K selbst. Das heißt*

$$Q(\mathfrak{o}_k) = (\mathfrak{o}_K \setminus \{0\})^{-1}\mathfrak{o}_k \simeq K.$$

Beweis.

1. Das $\mathfrak{o}_K$ ein Integritätsbereich ist, ist völlig klar, da $\mathfrak{o}_K \subseteq K$ ein Unterring ist und K ein Körper. (Daher wenn $xy = 0$ in $\mathfrak{o}_K$, dann gilt auch $xy = 0$ in K.)
2. Laut Korollar 1.2.19 gibt es ein Ringhomomorphismus

$$\varphi : Q(\mathfrak{o}_K) \to K.$$

Dies ist injektiv laut Proposition 1.1.52. Surjektivität folgt von Lemma 2.3.9: Sei $\alpha \in K$ und $N \in \mathbb{N}$, so dass $N\alpha \in \mathfrak{o}_K$. Es ist klar, dass $\frac{N\alpha}{N} \in Q(\mathfrak{o}_K)$ und nach α abgebildet wird.

□

Lemma 2.3.12. *Sei $K = \mathbb{Q}$. Dann ist $\mathfrak{o}_K = \mathbb{Z}$.*

Beweis. Sei $\beta \in \mathbb{Q}$ ganzalgebraisch. Laut Proposition 2.3.3 ist das Minimalpolynom $\mathfrak{m}_\beta \in \mathbb{Z}[X]$ ganzzahlig. Korollar 1.3.31 besagt, dass $\mathsf{grad}(\mathfrak{m}_\beta) \leq [Q : Q] = 1$, was nun zusammen die Existenz eines $a \in \mathbb{Z}$, mit $\mathfrak{m}_\beta = x + a$ impliziert. Da bei Definition des Minimalpolynoms $\mathfrak{m}_\beta(\beta) = 0$ haben wir $\beta = -a \in \mathbb{Z}$ und wir haben $\mathbb{Z} \subseteq \mathfrak{o}_\mathbb{Q}$. Die andere Seite ist trivial, da für $n \in \mathbb{Z}$ wir einfach $\mathfrak{m}_n(x) = x - n$ nehmen können. □

Beispiel 2.3.13. Wir werden bald kennenlernen, wie man solche Sachen genau berechnet, aber hier ein paar Beispiele der Zahlenringe in deren "Basen" über $\mathbb{Z}$.

1) Sei $K = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1}) = \{a + bi \mid a, b \in \mathbb{Q}\}$ die Gaußschen Zahlen. Dann ist $\mathfrak{o}_K = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, das Ring der ganzen Gaußschen Zahlen.
2) Sei $K = \mathbb{Q}(\sqrt{2})$. Dann gilt $\mathfrak{o}_K = \mathbb{Z}[\sqrt{2}]$.
3) Sei $K = \mathbb{Q}(\sqrt{5})$. Dann gilt *nicht*, dass $\mathfrak{o}_K = \mathbb{Z}[\sqrt{5}]$. Es gilt $\mathfrak{o}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$! Hierzu merke man, dass $\mathfrak{m}_{\frac{1+\sqrt{5}}{2}} = \alpha^2 - \alpha - 1$ und daher ist $\frac{1+\sqrt{5}}{2} \in \mathfrak{o}_K$ ganzalgebraisch. Es kann aber nicht als eine $\mathbb{Z}$-lineare Kombination von 1 und $\sqrt{5}$ erhalten werden.

Proposition 2.3.14. *Sei K ein algebraischer Zahlenkörper.*

- *Für $\alpha \in \mathfrak{o}_K$ ist $\mathsf{N}(\alpha) \in \mathbb{Z}$ und $\mathsf{Sp}(\alpha) \in \mathbb{Z}$.*
- *Sei $\mathcal{B}$ eine Basis von K als $\mathbb{Q}$-Vektorraum und $\mathcal{B} \subseteq \mathfrak{o}_K$. Dann ist $\Delta(\mathcal{B}) \in \mathbb{Z} \setminus \{0\}$.*

Beweis. Laut Korollar 2.3.4 sind die Konjugierten von α ganzalgebraisch und Korollar 2.3.7 besagt, dass die Summe und das Produkt von ganzalgebraischen Zahlen wieder eine ganzalgebraische Zahl ist. Daher sind $\mathsf{N}(k) \coloneqq \prod_{i=1}^{d} \sigma_i(k)$ und $\mathsf{Sp}(k) \coloneqq \sum_{i=1}^{d} \sigma_i(k)$ wieder ganzalgebraische Zahlen. Proposition 2.2.3 sagt des weiteren aus, dass die Norm und die Spur rationale Zahlen sind. Wir wissen also, dass $\mathsf{N}(\alpha)$ und $\mathsf{Sp}(\alpha)$ ganzalgebraisch und rational sind, also in $\mathfrak{o}_{\mathbb{Q}}$ liegen. Lemma 2.3.12 sagt nun, dass $\mathsf{N}(\alpha) \in \mathbb{Z}$ und $\mathsf{Sp}(\alpha) \in \mathbb{Z}$.

Die Definition der Diskriminanten (2.2.11) sagt nun aus, dass $\Delta(\mathcal{B})$ die Determinante einer Matrix mit ganzzahligen Einträgen ist, also $\Delta(\mathcal{B}) \in \mathbb{Z}$. Das es nicht Null ist Korollar 2.2.23. □

Aufgaben

Aufgaben 7

Aufgabe 46 (1 Punkt). Finde alle n, so dass $\frac{1+\sqrt{n}}{2}$ ganzalgebraisch ist.

Aufgabe 47 (2 Punkte). Zeige, dass

$$x = \frac{1}{4}(1 + \sqrt{21} + \sqrt{33} - \sqrt{77})$$

ganzalgebraisch ist.

Aufgabe 48 (2 Punkte). Sei

$$c = \frac{1}{3^{4/3}} - \frac{1}{3^{2/3}}.$$

Stelle es als ein Bruch $\frac{a}{b}$ dar, wobei a Ganzalgebraisch ist und $b \in \mathbb{Z}$.

Aufgabe 49 (6 Punkte). Sei $\alpha \in \mathbb{C}$ mit $\mathfrak{m}_\alpha = x^3 - 7$ mit Basis

$$\mathcal{B} = \{1, \alpha, \alpha^2\}.$$

i) (1 Teilpunkt) Was ist die Diskriminante dieser Basis? (*Tipp: Alte Übungsblätter könnten helfen.*)

ii) (3 Teilpunkte, je $0,5$ Punkte): Was ist die Norm der folgenden Elemente: (*Tipp: Mit Formeln arbeiten ist hier einfacher, als Definition benutzen.*)

1. α^2,
2. $1 - \alpha$,
3. $1 + \alpha + \alpha^2$,
4. $1 + 2\alpha + 2\alpha^2$,
5. $1 + 2\alpha + 3\alpha^2$,
6. $2 + \alpha + 5\alpha^2$.

Aufgabe 50 (2 Punkte). Sei $f(x) = x^3 + ax^2 + bx + c$ irreduzibel mit α eine Nullstelle. Bestimme die Norm von

$$1 + \alpha + \alpha^2.$$

2.4 Ganzheitsbasis

Definition 2.4.1. Sei K eine algebraische Erweiterung von $\mathbb{Q}$. Eine $\mathbb{Q}$-Vektorraumbasis $\mathcal{B} = \{b_1, \dots, b_n\}$ von K heißt *Ganzheitsbasis* falls

$$\mathfrak{o}_K = \{\sum_{i=1}^{n} k_i b_i \mid k_i \in \mathbb{Z}\}.$$

Bemerkung 2.4.2. Man sieht direkt, dass alle $b_i, 1 \leq i \leq n$ zwangsweise ganzalgebraische Zahlen sein müssen. Umgekehrt stimmt dies jedoch nicht, wie man es in den folgenden Beispielen sieht.

Beispiel 2.4.3. Sei K ein Zahlenkörper und $\mathcal{B}$ eine $\mathbb{Q}$-Basis von K. Folgende sind Beispiele, die keine Ganzheitsbasen sind:

- Sei $K = \mathbb{Q}$ und $\mathcal{B} = \{\frac{1}{2}\}$, $\mathcal{C} = \{2\}$. Dann ist weder $\mathcal{B}$ noch $\mathcal{C}$ eine Ganzheitsbasis, da $\mathcal{B} \notin \mathfrak{o}_{\mathbb{Q}} = \mathbb{Z}$ und $\{2n \mid n \in \mathbb{Z}\} \neq \mathbb{Z} = \mathfrak{o}_{\mathbb{Q}}$.
- Sei $K = \mathbb{Q}(i)$ und $\mathcal{B} = \{1, 2i\}$. Dann ist $\mathcal{B}$ *keine* Ganzheitsbasis, da $i \in \mathfrak{o}_K$ es aber keine $n, m \in \mathbb{Z}$ gibt, mit $i \neq n + 2im$.
- Sei $K = \mathbb{Q}(\sqrt{5})$. Wie schon im Beispiel 2.3.13 angesprochen ist $\mathcal{B} = \{1, \sqrt{5}\}$ keine Ganzheitsbasis.

Folgende sind Beispiele von Ganzheitsbasen:

- Sei $K = \mathbb{Q}$. Dann ist $\mathcal{B} = \{-1\}$ eine Ganzheitsbasis.
- Sei $K = \mathbb{Q}(i)$. Dann ist $\mathcal{B} = \{1, i\}$ eine Ganzheitsbasis.
- Sei $K = \mathbb{Q}(\sqrt{5})$. Dann ist $\mathcal{B} = \left\{1, \frac{1+\sqrt{5}}{2}\right\}$ eine Ganzheitsbasis.

Wir wollen nun beweisen, dass es immer eine Ganzheitsbasis gibt und einen Weg geben, solch eine Basis zu finden. Die Idee ist, dass es irgendwie *minimal* sein soll. Wir können aber nicht einfach sagen, dass $\Delta(\mathcal{B})$ minimal sein soll, da wir dies a-priori beliebig klein machen können. Z.B., bei $K = \mathbb{Q}$ kann man $\mathcal{B} = \{\frac{1}{2}\}$, $\mathcal{B} = \{\frac{1}{3}\}$, $\mathcal{B} = \{\frac{1}{4}\}$, ... wählen. Was wir zusätzlich wollen, ist, dass die Basis in $\mathfrak{o}_K$ landet, denn dann wird $\Delta(\mathcal{B}) \in \mathbb{Z}$ sein (Proposition 2.3.14).

Dies können wir mithilfe von Lemma 2.3.9 machen. Zu jeder $\mathbb{Q}$-Basis $\mathcal{B}$ eines Zahlenkörpers K finden wir eine Basis $\mathcal{C}$ indem wir jeden $\alpha \in \mathcal{B}$ mit einem entsprechen $N_\alpha \in \mathbb{N}$ multiplizieren um in $\mathfrak{o}_K$ zu landen. (Da die Basis endlich ist, kann man sogar einen einzigen $N \in \mathbb{N}$ finden). Dies führt uns zur folgenden Aussage:

Satz 2.4.4. *Für jeden Zahlenkörper K ist eine $\mathbb{Q}$-Basis $\mathcal{B}$ mit der Eigenschaft, dass*

1) $\mathcal{B} \subseteq \mathfrak{o}_K$ und

2) $|\Delta(\mathcal{B})| \leq |\Delta(\mathcal{C})|$ für jede andere $\mathbb{Q}$-Basis $\mathcal{C}$ von K mit der Eigenschaft $\mathcal{C} \subseteq \mathfrak{o}_K$

erfüllt werden, eine Ganzheitsbasis. Spezifisch: Jedes Zahlenkörper hat (mindestens) eine Ganzheitsbasis.

Beweis. Sei $\mathcal{B} =: \{e_1, \dots, e_n\}$ wie in der Aussage des Satzes. Von Teil 1) der Annahme $\mathcal{B} \subseteq \mathfrak{o}_K$, gilt

$$\sum_{i=1}^{n} k_i e_i \subseteq \mathfrak{o}_K,$$

wobei $k_i \in \mathbb{Z}$ für jeden $1 \leq i \leq n$. Wenn $\sum_{i=1}^{n} k_i e_i = \mathfrak{o}_K$, sind wir fertig. Wenn nicht, gibt es eine ganzalgebraische Zahl $\alpha = \sum_{i=1}^{n} r_i e_i \in \mathfrak{o}_K$, so dass $r_i \in \mathbb{Q}$ und mindestens einer ist nicht in $\mathbb{Z}$ liegt.

Da die ganzalgebraischen Zahlen einen Ring formen (also unter Subtraktion abgeschlossen sind), können wir, nach Abzug (bzw. Addition) einer geeigneten ganzalgebraischen Zahl, annehmen, dass $0 \leq r_i < 1$, für jeden $1 \leq i \leq n$. Da $0 \in \mathbb{Z}$, gilt (nach umordnen) $r_1 \neq 0$.

Sei $\mathcal{C} \coloneqq \{\alpha, e_2, \dots, e_n\}$. Wir wollen jetzt 2 Sachen zeigen. Erstens, dass $\mathcal{C}$ eine $\mathbb{Q}$-Basis von K ist mit $\mathcal{C} \subseteq \mathfrak{o}_K$ und zweitens, dass $|\Delta(\mathcal{C})| < |\Delta(\mathcal{B})|$. Dies wird wegen dem zweiten Teil der Annahme zum Widerspruch führen und so den Satz beweisen.

1. Die Tatsache, dass $\mathcal{C} \subseteq \mathfrak{o}_K$ is klar. Wir wollen zeigen, dass $\alpha, e_2, \dots, e_n$ linear unabhängig sind. Aus Dimensionsgründen ($\#|\mathcal{B}| = \#|\mathcal{C}|$) wird $\mathcal{C}$ dann eine Basis von K als $\mathbb{Q}$-Vektorraum bilden. In anderen Worten, wir wollen zeigen, dass $\det(\mathcal{C}) \neq 0$. Es gilt

$$\mathcal{C} = T\mathcal{B},$$

wobei

$$T = \begin{bmatrix} r_1 & 0 & 0 & \cdots 0 \\ r_2 & 1 & 0 & \cdots 0 \\ r_3 & 0 & 1 & \cdots 0 \\ \vdots & & \vdots & \vdots \\ r_n & 0 & 0 & \cdots 1 \end{bmatrix}$$

die Basiswechselmatrix ist. Da $\det(T) = r_1$ und $r_1 \neq 0$ folgt die Annahme.

2. Korollar 2.2.18 sagt uns, dass

$$\Delta(\mathcal{C}) = \det(T)^2 \Delta(\mathcal{B}) = r_1^2 \Delta(\mathcal{B}).$$

Da, bei Annahme, $r_1 \neq 0$ und $0 \leq r_i < 1$, folgt, $0 < r_1 < 1$ und daher,

$$|\Delta(\mathcal{C})| = |r_1^2||\Delta(\mathcal{B})| < |\Delta(\mathcal{B})|.$$

□

Korollar 2.4.5. *Sei K ein algebraischer Zahlenkörper. Dann gilt*

$$\mathfrak{o}_K \simeq \mathbb{Z}^k$$

als Abelsche Gruppen.

Beweis. Dies ist quasi die Definition einer Ganzheitsbasis, das jedes Element auf eine einzige Art und Weise als eine lineare Kombination der Basiselemente über $\mathbb{Z}$ dargestellt werden können. □

Bemerkung 2.4.6. Natürlich gilt diese Gleichung nicht als Ringe, nur auf der Stufe der Gruppen ($\mathbb{Z}$-Module).

Korollar 2.4.7. *Sei $I \subseteq \mathfrak{o}_K$. Dann ist $I \simeq \mathbb{Z}^l$, mit $l \in \mathbb{N}$ eine freie abelsche Gruppe.*

Beweis. Wir benutzen hier die bekannte Tatsache, dass eine Untergruppe einer freien abelschen Gruppe frei ist. □

2.4.1 Algorithmus zum finden einer Ganzheitsbasis

Der Beweis des Satzes gibt uns einen Algorithmus um eine Ganzheitsbasis zu finden.

1. Nimm eine $\mathbb{Q}$-Basis von K.
2. Multiplizieren die Basiselemente mit geeigneten $N_\alpha \in \mathbb{N}$ um diese ganzalgebraisch zu machen. Lass diese neue Basis $\mathcal{B} = \{b_1, \dots, b_d\} \subseteq \mathfrak{o}_K$ sein.
3. Berechne $\Delta(\mathcal{B})$ und lass $N \in \mathbb{N}$ die größte natürliche Zahl sein, so dass N^2 die Diskriminante $\Delta(\mathcal{B})$ teilt.
4. Für jedes Element der Form

$$\alpha \coloneqq \sum_{i=0}^{d-1} \frac{1}{N} a_i b_i, \quad a_i \in \{0, \dots, N-1\},$$

bestimme, ob α ganzalgebraisch ist. (Also, ob $\alpha \in \mathfrak{o}_K$).

5. Wenn eines dieser Elemente ganzalgebraisch ist, wechsle eines der e_i mit α aus und wiederhole von Schritt 3 vorwärts.

6. Wenn keines der Elemente, wie in Schritt 4. konstruiert, ganzalgebraisch ist (oder, wenn $N = 1$ die größte Zahl ist, dessen Quadrat $\Delta(\mathcal{B})$ teilt), ist die konstruierte Basis ganzalgebraisch.

Um den Algorithmus 2.4.1 oben Sinn zu geben, muss man das folgende Lemma beweisen:

Lemma 2.4.8. *Wenn kein Element der Form $\alpha := \sum_{i=0}^{d-1} \frac{1}{N} a_i b_i, \quad a_i \in \{0, \dots, N-1\}$ ganz ist (mit N wie im Algorithmus 2.4.1), kann auch kein Element der Form $\beta := \sum_{i=0}^{d-1} r_i b_i, \quad a_i \in \mathbb{Q}$ ganz sein.*

Beweis. Sei $\beta = \sum_{i=0}^{d-1} r_i b_i,\ a_i \in \mathbb{Q}$ ganz, mit $0 \neq r_j = \frac{s}{t}$ gekürzt. Indem wir b_j mit β ersetzen, erhalten wir eine neue Basis $\mathcal{C} := \{b_1, b_2, \dots, b_{j-1}, \beta, b_{j+1}, \dots, b_d\}$, welches freilich auch eine Teilmenge von $\mathfrak{o}_K$ ist. Wie im Beweis von Satz 2.4.4 argumentiert, gilt $|\Delta(\mathcal{C})| = r_j^2 \mid \Delta(\mathcal{B})|$. Da N die größte ganze Zahl ist, dessen Quadrat $\Delta(\mathcal{B})$ teilt, gilt $\Delta(\mathcal{B}) = N^2 m$, mit $m \in \mathbb{N}$ quadratfrei. Es folgt

$$\frac{s^2}{t^2} = r_j^2 = \frac{|\Delta(\mathcal{C})|}{|\Delta(\mathcal{B})|} = \frac{|\Delta(\mathcal{C})|}{|N^2 m|},$$

woraus wir $t^2 \mid N^2 m$ schließen können, da $r_j = \frac{s}{t}$ gekürzt war. Aufgepasst, wir können nicht $t^2 = N^2 m$ schließen, da $\frac{|\Delta(\mathcal{C})|}{|\Delta(\mathcal{B})|}$ nicht gekürzt sein muss. Teilbarkeit aber folgt direkt. Aus $t = p_1^{e_1} \cdots p_r^{e_r}$ Primdarstellung folgt $t^2 = p_1^{2e_1} \cdots p_r^{2e_r}$. Da aber m nicht durch eine Quadratzahl teilbar ist, muss $p_1^{2e_1 - 1} \cdots p_r^{2e_r - 1}$ die Zahl N^2 teilen. Da aber $p_j^{2e_j - 1} \mid N^2$ muss N^2, wenn man es als Produkt von Primzahlen darstellt, p_j mit mindestens Potenz $2e_j - 1$ erhalten. Da es aber eine Quadratzahl ist und daher jede Primzahl mit einer geraden Potenz erhält, muss p_j mit mindestens Potenz $2e_j$ erhalten. Daher, muss N die Primzahl p_j mit mindestens Grad e_j erhalten. Da dies für alle Primfaktoren von t gilt, folgt $t \mid N$ und daher auch $t \leq N$.

Dies gilt für alle Koeffizienten r_i von β und daher ist es von der Form α. □

Beispiel 2.4.9. Das folgende Beispiel wird in Satz 2.4.16 im allgemeinen gemacht. Es ist auch nicht viel schwerer. Hier kann man es sich aber, für spezifische Zahlen, durchlesen. Sein $K = \mathbb{Q}(\sqrt{-2})$ und $L = \mathbb{Q}(\sqrt{-3})$. Wir wollen die Ganzheitsbasen bestimmen. Wir gehen wie im Algorithmus voran:

1. Wir nehmen die $\mathbb{Q}$-Basen $\mathcal{B} = \{1, \sqrt{-2}\}$ und $\mathcal{C} = \{1, \sqrt{-3}\}$ von K und L respektive.

2. Diese Basen sind schon ganzalgebraisch. Hierfür überprüfe man die Minimalpolynome $\mathfrak{m}_{\sqrt{-2}} = x^2 + 2$ und $\mathfrak{m}_{\sqrt{-3}} = x^2 + 3 \in \mathbb{Z}[X]$.

3. Wir benutzen die Formel von Korollar 2.2.22 (das Konjugierte zu $\sqrt{n}$ ist natürlich $-\sqrt{n}$) und erhalten direkt, dass $\Delta(\mathcal{B}) = \left(\sqrt{-2} - \left(-\sqrt{-2}\right)\right)^2 = (2\sqrt{-2})^2 = -8$ und $\Delta(\mathcal{C}) = \left(\sqrt{-3} - \left(-\sqrt{-3}\right)\right)^2 = (2\sqrt{-3})^2 = -12$. In beiden Fällen ist $N = 2$ die größte natürliche Zahl, dessen Quadrat die Diskriminante teilt.

4. Es gilt die Elemente

$$\alpha_1 = \frac{1}{2},\ \alpha_2 = \frac{\sqrt{-2}}{2},\ \alpha_3 = \frac{1}{2}\left(1 + \sqrt{-2}\right) \quad (\text{ für } \Delta(\mathcal{B}) \text{ })$$

und

$$\beta_1 = \frac{1}{2},\ \beta_2 = \frac{\sqrt{-3}}{2},\ \beta_3 = \frac{1}{2}\left(1 + \sqrt{-3}\right) \quad (\text{ für } \Delta(\mathcal{C}) \text{ })$$

auf Ganzheit zu überprüfen.

Es ist klar, dass α_1 und β_1 nicht ganzalgebraisch sind, da deren Minimalpolynome $x - \frac{1}{2}$ ist. Bei den anderen Elementen berechnen wir zuerst die Norm, da laut Proposition 2.3.14 ein

Element nicht ganzalgebraisch sein kann, wenn dessen Norm nicht in $\mathbb{Z}$ liegt. Wir benutzen wiederholt Proposition 2.2.6, Korollar 2.2.10 und Lemmas 2.2.8 2.2.9.

Wir haben

$$\begin{aligned}
\mathsf{N}(\alpha_2) &= \mathsf{N}\left(\frac{\sqrt{-2}}{2}\right) = \mathsf{N}\left(\frac{1}{2}\right)\mathsf{N}(\sqrt{-2}) = \frac{1}{4}\cdot(-1)^2\cdot 2 = \frac{1}{2}\\
\mathsf{N}(\alpha_3) &= \mathsf{N}\left(\frac{1+\sqrt{-2}}{2}\right) = \mathsf{N}\left(-\frac{1}{2}\right)\mathsf{N}\left(-1-\sqrt{-2}\right) = \left(-\frac{1}{2}\right)^2 \mathfrak{m}_{\sqrt{-2}}(-1) = \frac{1}{4}\left((-1)^2+2\right) = \frac{3}{4}\\
\mathsf{N}(\beta_2) &= \mathsf{N}\left(\frac{\sqrt{-3}}{2}\right) = \mathsf{N}\left(\frac{1}{2}\right)\mathsf{N}\left(\sqrt{-3}\right) = \frac{1}{4}\cdot(-1)^2\cdot 3 = \frac{3}{4}\\
\mathsf{N}(\beta_3) &= \mathsf{N}\left(\frac{1+\sqrt{-3}}{2}\right) = \mathsf{N}\left(-\frac{1}{2}\right)\mathsf{N}\left(-1-\sqrt{-3}\right) = \left(-\frac{1}{2}\right)^2 \mathfrak{m}_{\sqrt{-3}}(-1) = \frac{1}{4}\left((-1)^2+3\right) = \frac{4}{4} = 1.
\end{aligned}$$

Als solches ist nur $\beta_3 \in \mathbb{Z}$. Wir können also schon direkt schlussfolgern, dass $\mathcal{B}$ eine Ganzheitsbasis ist. Bei $\mathcal{C}$ muss man aber weitermachen. Wir müssen nun weiter erforschen, ob β_3 wirklich ganzalgebraisch ist. Zur Erinnerung, Proposition 2.3.14 ist *keine* genau-dann Aussage. Daher, auch nicht-algebraische Elemente können ganzzahlige Normen haben. Wir berechnen das Minimalpolynom von β_3: Es gilt $2\beta_3 - 1 = \sqrt{-3}$, woraus $4\beta_3^2 - 4\beta_3 + 1 = -3$ und daher $\beta_3^2 - \beta_3 + 1 = 0$ folgt. Das Minimalpolynom ist daher

$$\mathfrak{m}_{\beta_3} = x^2 - x + 1,$$

was natürlich $\beta_3 \in \mathfrak{o}_L$ impliziert.

5. Wir gehen zu Schritt 3, aber nun mit der Basis $\mathcal{C}' := \{1, \beta_3\} = \{1, \frac{1+\sqrt{-3}}{2}\}$.

   [5.4] Wir berechnen die Diskriminante von $\mathcal{C}'$. Auch hier können wir Formel 2.2.22 benutzten, da natürlich $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\beta_3)$. Das Konjugierte zu β_3 ist $\frac{1-\sqrt{-3}}{2}$, was uns

$$\Delta(\mathcal{C}') = \left(\frac{1+\sqrt{-3}}{2} - \frac{1-\sqrt{-3}}{2}\right)^2 = \left(\frac{(1+\sqrt{-3}) - (1-\sqrt{-3})}{2}\right)^2 = \left(\sqrt{-3}\right)^2 = -3$$

   gibt. Als solches ist $N = 1$ die größte ganze Zahl, dessen Quadrat $\Delta(\mathcal{C}')$ teilt und somit ist $\mathcal{C}'$ ein Ganzheitsbasis.

Wir fassen unsere Diskussion zusammen und sagen $\mathfrak{o}_K = \mathbb{Z}\left[\sqrt{-2}\right]$, $\mathfrak{o}_L = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

Proposition 2.4.10. *Im Algorithmus im Abschnitt 2.4.1 reicht es aus für Primzahlen zu überprüfen, ob dessen Quadrat die Diskriminante $\Delta(\mathcal{B})$ teilt.*

Beweis. Sei $\alpha = \sum_{i=0}^{d-1} \frac{1}{N} a_i e_i$ ganzalgebraisch mit $0 \le a_i \le N-1$. Zuerst können wir annehmen, dass $(N, a_1, \ldots, a_{d-1}) = (1)$, in anderen Worten, dass N und alle a_i's zusammen, teilerfremd sind. Sei nämlich $N = qN'$ und gelte $a_i = qa_i'$ für alle $1 \le i \le d-1$. Dann können wir schreiben

$$\alpha = \sum_{i=0}^{d-1} \frac{1}{N} a_i e_i = \sum_{i=0}^{d-1} \frac{1}{qN'} qa_i' e_i = \sum_{i=0}^{d-1} \frac{1}{N'} a_i' e_i.$$

Da $0 \le a_i \le N-1$, also $0 \le qa_i' \le qN'-1$, haben wir natürlich $0 \le a_i' \le N'-1$, was unsere Reduktion ergibt.

Sei $1 \ne p \mid N$ ein Teiler, also $N = pk$ und gelte $\alpha = \sum_{i=0}^{d-1} \frac{1}{pk} a_i e_i$. Dann ist

$$k\alpha = \sum_{i=0}^{d-1} \frac{1}{p} a_i e_i, \quad 0 \le a_i \le pk-1$$

auch ganzalgebraisch (da $k \in \mathbb{Z} \subseteq \mathfrak{o}_K$). Jeden der Koeffizienten a_j können wir schreiben als $a_j = np + a'_j$, mit $n \in \mathbb{N}$ und $0 \leq a'_j \leq p-1$. Da die Elemente $\frac{1}{p}npe_i = ne_i \in \mathfrak{o}_K$ ganzalgebraisch sind können wir einen $\theta \in \mathfrak{o}_K$ finden, so dass

$$k\alpha - \theta = \sum_{i=0}^{d-1} \frac{1}{p} a'_i e_i \quad 0 \leq a'_i \leq p-1 \mathfrak{o}_K.$$

Das Element α bzw. $\alpha' := k\alpha - \theta = 0$ ist genau dann Null, wenn alle Koeffizienten a_i bzw. a'_i Null sind. Bei Definition von a'_i passiert dies genau dann, wenn alle a_i's durch p teilbar sind. Dann wäre aber $(N, a_1, \ldots, a_{d-1}) = (p)$, was unserer Annahme widerspricht.

Als solches können wir für $\alpha \neq 0$ schlussfolgern, dass $\alpha' \neq 0$ und indem wir einen der Basiselemente mit α' ersetzen, wird die Diskriminante auch echt kleiner. Als solches reicht es aus, die nur für die Teiler von N zu überprüfen, spezifisch also nur für Primzahlen. □

Bemerkung 2.4.11. Falls es das Argument von Proposition 2.4.10 klarer macht, kann man die Reduktion auch so verstehen: Wenn q ein echter Teiler von N ist (also $q \neq 1$ und $q \neq N$), dann ist N' auch ein echter Teiler. Als solches könnten wir α schon mit einem Teiler von N finden, nämlich mit N' (anstelle von q, bzw. p, wie im weiteren Teil des Arguments). In diesem Fall ist $\alpha' = \alpha$.

Bemerkung 2.4.12. Wenn, z. B., $N = pq$ die Primfaktorzerlegung ist und der Grad der Erweiterung 2, müssen wir ohne diesen Lemma $(pq)^2 - 1$ Fälle ansehen. Mit der obigen Vereinfachung jedoch, braucht man nur $(p^2-1) + (q^2-1)$ Elemente überprüfen. Das heißt, wir müssten

$$(p^2-1)(q^2-1)$$

weniger Fälle untersuchen. Bei Grad 3 wäre es schon $(p^3-1)(q^3-1)$. Desto größer der Grad und desto mehr Primfaktoren, desto größer wird der Unterschied´.

Bemerkung 2.4.13. Aufgepasst, wenn $p^2 \mid N$ (daher $p^4 \mid \Delta(\mathcal{B})$), reicht es nicht aus, nur für p zu überprüfen. Dann sollte man zuerst für p überprüfen und wenn man so eine kleinere Basis $\mathcal{C}$ findet, muss man dies nochmal für p testen. Dies ist aber immer noch einfacher, als für p^2 direkt zu testen, sogar für $p = 2$.

2.4.2 Ganzheitsbasen von quadratischen Körpern

Im Beispiel 2.4.9 haben wir gesehen, dass die Ganzheitsbasis von $\mathbb{Q}(\sqrt{-2}) = \{1, \sqrt{-2}\}$ ist, aber für $\mathbb{Q}(\sqrt{-3})$ ist es $\left\{1, \frac{1+\sqrt{-3}}{2}\right\}$. In diesem Abschnitt wollen wir eine Formel für alle quadratischen Körpererweiterungen von $\mathbb{Q}$ geben.

Definition 2.4.14. Eine Körpererweiterung K von $\mathbb{Q}$ heißt *quadratisch*, wenn $[K : \mathbb{Q}] = 2$.

Von Aufgabe 39 wissen wir, dass jede quadratische Erweiterung K von $\mathbb{Q}$ von der Form $K = \mathbb{Q}(\sqrt{r})$ ist, mit $r \in \mathbb{Q}^*$, quadratfrei. Auf der anderen Seite ist $[\mathbb{Q}(\sqrt{r}) : \mathbb{Q}] = 2$, für $r \in \mathbb{Q}^*$, quadratfrei, da das Minimalpolynom $\mathfrak{m}_{\sqrt{r}} = x^2 - r$ ist.

Wir fassen unsere Diskussion zusammen indem wir sagen:

Proposition 2.4.15. *Die quadratischen Körpererweiterungen sind genau von der Form $\mathbb{Q}(\sqrt{n})$, wobei $n \in \mathbb{Z}$ quadratfrei ist.*

Satz 2.4.16. *Sei $n \in \mathbb{Z}$ quadratfrei und $K = \mathbb{Q}(\sqrt{n})$.*

- *Für $n \not\equiv 1 \mod 4$ ist $\mathcal{B} := \{1, \sqrt{n}\}$ eine Ganzheitsbasis von K.*
- *Für $n \equiv 1 \mod 4$ ist $\mathcal{B}' := \left\{1, \frac{1+\sqrt{n}}{2}\right\}$ eine Ganzheitsbasis von K.*

Beweis. Es ist klar, dass $\mathcal{B} = \{1, \sqrt{n}\}$ eine $\mathbb{Q}$-Basis von K ist und das $\mathcal{B} \subseteq \mathfrak{o}_K$. Wir wollen untersuchen, wann $\mathcal{B}$ eine Ganzheitsbasis ist. Wie im Algorithmus im Abschnitt 2.4.1, berechnen wir die Diskriminante der Basis $\mathcal{B}$. Man kann dies frei nach belieben mit Proposition 2.2.12,

Korollar 2.2.22 oder Satz 2.2.24 machen. Wir haben $\Delta(\mathcal{B}) = 4n$. Nach Annahme ist n quadratfrei. Daher ist $N = 2$ die größte Quadratzahl die $4n$ teilt. Wie im Schritt 4, bestimmen wir ob folgende Elemente

$$\alpha_1 = \frac{1}{2} \quad (a_1 = 1, a_2 = 0) \qquad \alpha_2 = \frac{\sqrt{n}}{2} \quad (a_1 = 0, a_2 = 1) \qquad \alpha_3 = \frac{1+\sqrt{n}}{2} \quad (a_1 = 1, a_2 = 1)$$

ganzalgebraisch sind. Es ist klar, dass $\frac{1}{2} \notin \mathfrak{o}_k$. Die Norm von $\frac{\sqrt{n}}{2}$ ist

$$\mathsf{N}\left(\frac{\sqrt{n}}{2}\right) = \frac{-n}{4}.$$

Da n quadratfrei ist, gilt $\frac{-n}{4} \notin \mathbb{Z}$ und Proposition 2.3.14 impliziert daher, dass $\frac{\sqrt{n}}{2}$ nicht ganzalgebraisch ist. Letztens sehen wir uns

$$\mathsf{N}\left(\frac{1+\sqrt{n}}{2}\right) = \frac{1-n}{4}$$

an. Jetzt gibt es die zwei Möglichkeiten der Annahme.

- Zuerst, sei $n \not\equiv 1 \mod 4$. Dann ist $\frac{1-n}{4} \notin \mathbb{Z}$ und $\mathcal{B}$ ist eine Ganzheitsbasis.
- Im Fall wenn $n \equiv 1 \mod 4$ ist, ist das Bruch $\frac{1-n}{4}$ eine ganze Zahl sein. Daher müssen wir dessen Minimalpolynom untersuchen, um zu bestimmen, ob es wirklich ganzalgebraisch ist. Wir haben $\left(\alpha_3 - \frac{1}{2}\right)^2 = \frac{n}{4}$. Ausmultipliziert und umgeordnet ergibt es $\alpha_3^2 - \alpha_3 + \frac{1-n}{4} = 0$. Betrachte das Polynom
$$\mathfrak{m}_{\alpha_3} := x^2 - x + \frac{1-n}{4}.$$
Da $1 - n \equiv 0 \mod 4$, ist $\frac{1-n}{4} \in \mathbb{Z}$ und als solches gilt, $\mathfrak{m}_{\alpha_3} \in \mathbb{Z}[X]$. Wir haben $\mathfrak{m}_{\alpha_3}(\alpha_3) = 0$ und die Definition einer ganzalgebraischen Zahl ergibt nun, dass $\alpha_3 \in \mathfrak{o}_K$. Wir definieren die neue Basis (Schritt 5 im Algorithmus) $\mathcal{B}' := \left\{1, \frac{1+\sqrt{n}}{2}\right\}$. Es gilt $\Delta(\mathcal{B}') = n$, was quadratfrei ist und daher, eine Ganzheitsbasis.

□

2.4.3 Ganzheitsbasen von kubischen Körpern

Definition 2.4.17. Ein algebraischer Zahlenkörper K heißt *kubisch* wenn $[K : \mathbb{Q}] = 3$.

Proposition 2.4.18. *Sei K ein kubischer Zahlenkörper. Dann ist K von der Form $\mathbb{Q}(\alpha)$, wobei α eine Nullstelle eines irreduziblen Polynoms der Form*

$$\mathfrak{m}_\alpha(x) = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

ist.

Beweis. Laut Satz 2.1.4 und Beispiel 1.3.28 wissen wir, dass $K = \mathbb{Q}(\theta)$, wobei θ eine Nullstelle eines Polynom on Grad 3 ist. Daher

$$\mathfrak{m}_\theta(x) = x^3 + ux^2 + vx + w.$$

(Leitkoeffizient können wir gleich 1 setzen, da wir über einen Körper sind). Nun müssen wir zwei Vereinfachungen machen: 1. Den Koeffizient von x^2 loswerden, 2. Die Koeffizienten ganzzahlig machen.
Vereinfachung 1: Wir machen den Variablenwechsel

$$x \mapsto x - \frac{u}{3}$$

und erhalten

$$\begin{aligned}\mathfrak{m}_\theta\left(x-\frac{u}{3}\right) &= \left(x-\frac{u}{3}\right)^3+u\left(x-\frac{u}{3}\right)^2+v\left(x-\frac{u}{3}\right)+w\\ &= x^3+(-u+u)\,x^2+\left(\frac{u^2}{3}-2\frac{u^2}{3}+v\right)x+\left(-\frac{u^3}{27}+\frac{u^3}{9}-\frac{uv}{3}+w\right)\\ &= x^3+\left(v-\frac{u^2}{3}\right)x+\left(\frac{2u^3}{9}\frac{uv}{3}+w\right).\end{aligned}$$

Wir benutzen die Notation

$$\alpha=\theta-\frac{u}{3},\quad a=\left(v-\frac{u^2}{3}\right)\quad\text{und}\quad b=\left(\frac{2u^3}{9}\frac{uv}{3}+w\right).$$

Daher können wir annehmen, dass das Koeffizient von x^2 gleich Null ist.

Der zweite Teil wurde im Korollar 2.3.10 bewiesen. □

Definition 2.4.19. Ein kubisches Polynom der Art

$$f(x)=x^3+ax+b$$

wir *normiert* genannt.

Proposition 2.4.20. *Sei $K=\mathbb{Q}(\alpha)$, mit*

$$\mathfrak{m}_\alpha(x)=x^3+ax+b,\quad a,b\in\mathbb{Q}$$

und $\mathcal{A}=\{1,\alpha,\alpha^2\}$. Dann gilt

$$\Delta(\mathcal{A})=-27b^2-4a^3.$$

Beweis. Dies wurde in Aufgabe 45 bewiesen. Hier ein alternativer Beweis, welches Satz 2.2.24 benutzt, um die Rechnung etwas zu vereinfachen.

Wir haben

$$\mathfrak{m}'_\alpha(x)=3x^2+a$$

woraus

$$\Delta(\mathcal{A})=(-1)^3\mathsf{N}(3\alpha^2+a)=-(3\alpha_1^2+a)(3\alpha_2^2+a)(3\alpha_3^2+a)$$

folgt. Hier sind $\alpha=\alpha_1,\alpha_2,\alpha_3$ die Konjugierten von α. Ausmultipliziert ist dies

$$\Delta(\mathcal{A})=-27(\alpha_1\alpha_2\alpha_3)^2-9a(\alpha_1^2\alpha_2^2+\alpha_1^2\alpha_3^2+\alpha_2^2\alpha_3^2)-3a^2(\alpha_1^2+\alpha_2^2+\alpha_3^2)-a^3.$$

Wir haben

$$s_1(\alpha)=\alpha_1+\alpha_2+\alpha_3=0,\ s_2(\alpha)=\sum\alpha_i\alpha_j=a\quad\text{und}\quad s_3(\alpha)=\alpha_1\alpha_2\alpha_3=-b.$$

Dies impliziert

$$\begin{aligned}\alpha_1^2\alpha_2^2\alpha_3^2 &= s_3^2=b^2\\ \alpha_1^2\alpha_2^2+\alpha_1^2\alpha_3^2+\alpha_2^2\alpha_3^2 &= s_2^2-2s_1s_3=a^2\\ \alpha_1^2+\alpha_2^2+\alpha_3^2 &= s_1^2-2s_2=-2a.\end{aligned}$$

Also solches gilt

$$\Delta(\mathcal{A})=-27b^2-9a^3+6a^3-a^3=-27b^2-4a^3.$$

□

Beispiel 2.4.21. Sei $\alpha = \sqrt[3]{2}$ und $K = \mathbb{Q}(\alpha)$. Wir wollen beweisen, dass die Ganzheitsbasis von K die Menge $\mathcal{B} = \{1, \alpha, \alpha^2\}$ ist.

Das $\mathcal{B}$ eine $\mathbb{Q}$-Basis von K ist, ist völlig klar. Das $\mathcal{B} \subseteq \mathfrak{o}_K$ ist auch direkt ersichtlich da $\mathfrak{m}_\alpha = x^3 - 2$. Wir berechnen die Diskriminante

$$\Delta(\mathcal{B}) = -27 \cdot 4 = -108.$$

Daher sind $p = 2$ und $q = 3$ beide Primzahlen, dessen Quadrate die Diskriminante teilen.

$\underline{p = 2}$. Wir haben die Elemente

$$\nu_i = \sum_{i=0}^{2} \frac{a_i \alpha^i}{2}, \quad a_i \in \{0, 1\}$$

auf Ganzalgebraität zu untersuchen. Ausgeschrieben, mit ihrer Norm, sind es

Elementname	Element	Norm	Koeffiziente
ν_1 :	$\frac{\alpha^2}{2}$	$\frac{4}{8} = \frac{1}{2}$	$a_0 = 0, a_1 = 0, a_2 = 1$
ν_2 :	$\frac{\alpha}{2}$	$\frac{2}{8} = \frac{1}{4}$	$a_0 = 0, a_1 = 1, a_2 = 0$
ν_3 :	$\frac{\alpha+\alpha^2}{2}$	$\frac{6}{8} = \frac{3}{4}$	$a_0 = 0, a_1 = 1, a_2 = 1$
ν_4 :	$\frac{1}{2}$	$\frac{1}{8}$	$a_0 = 1, a_1 = 0, a_2 = 0$
ν_5 :	$\frac{1+\alpha^2}{2}$	$\frac{5}{8}$	$a_0 = 1, a_1 = 0, a_2 = 1$
ν_6 :	$\frac{1+\alpha}{2}$	$\frac{3}{8}$	$a_0 = 1, a_1 = 1, a_2 = 0$
ν_7 :	$\frac{1+\alpha+\alpha^2}{2}$	$\frac{1}{8}$	$a_0 = 1, a_1 = 1, a_2 = 1$

Hier haben wir Korollar 2.2.10 angewandt, um die Norm von α direkt zu bestimmen, was uns auch die Norm von α^2 (von $1 = \alpha^0$) und die Norm von $2 = \alpha^3$, daher auch die Norm von $\frac{1}{2}$ gibt. Lemma 2.2.9 für $r = -1$ erlaubt uns die Norm von $1 + \alpha$ und $\alpha + \alpha^2$ zu berechnen.

Da wir die Norm von $1+\alpha$ schon kennen und mit Lemma 2.2.9 die Norm von $\alpha+2$ bestimmen können, wissen wir auch die Norm von $1 + \alpha^2$, denn $(1 + \alpha^2)\alpha = \alpha + 2$.

Letztendlich haben wir auch $(1 + \alpha + \alpha^2)(1 - \alpha) = -1$, was uns die Norm von ν_7 berechnen lässt.

Es ist klar, dass keines der ν_i's ganzalgebraisch ist, daher müssen wir soweit nichts in der Basis $\mathcal{B}$ ersetzen.

$\underline{q = 3}$. Wir haben die Elemente

$$\mu_i = \sum_{i=0}^{2} \frac{a_i \alpha^i}{3}, \quad a_i \in \{0, 1, 2\}$$

auf Ganzalgebraität zu untersuchen. Ausgeschrieben, mit deren Normen sind diese auf Seite 65.

Hierzu verwenden wir die Resultate von dem vorigen Fall für rund die Hälfte. Für die Andere benutzen wir folgende Tatsachen: $(1 + 2\alpha) = -2(-\frac{1}{2} - \alpha) = -2\mathfrak{m}_\alpha(-\frac{1}{2})$, $(\alpha + 2\alpha^2) = \alpha(1 + 2\alpha)$, $(1 + 2\alpha^2)\alpha = (4 + \alpha) = -\mathfrak{m}_\alpha(-4)$, $(2 + \alpha^2)\alpha = 2\alpha + 2 = 2(\alpha + 1)$, $(2 + \alpha + \alpha^2) = (1 + \alpha + \alpha^2)\alpha$, $(2+2\alpha+\alpha^2) = (1+\alpha+\alpha^2)\alpha^2$, $(1+2\alpha+\alpha^2) = (1+\alpha)^2$, $(1+\alpha+2\alpha^2)(1-\alpha)\alpha = 3(\frac{2}{3}-\alpha) = 3\mathfrak{m}_\alpha(\frac{2}{3})$, $(1 + 2\alpha + 2\alpha^2)(1 - \alpha) = (-3 + \alpha) = -\mathfrak{m}_\alpha(3)$, und $(2 + \alpha + 2\alpha^2)(1 - 2\alpha) = (-6 - 3\alpha) = 3\mathfrak{m}_\alpha(-2)$.

Resultat: Da auch hier keines der Normen in $\mathbb{Z}$ liegen, ist die Basis $\mathcal{B} = \{1, \alpha, \alpha^2\}$ eine Ganzheitsbasis, daher haben wir

$$\mathfrak{o}_K = \mathbb{Z}[\alpha].$$

Elementname	Element	Norm	Koeffiziente
μ_1 :	$\frac{\alpha^2}{3}$	$\frac{4}{27}$	$a_0 = 0, a_1 = 0, a_2 = 1$
μ_2 :	$\frac{2\alpha^2}{3}$	$\frac{32}{27}$	$a_0 = 0, a_1 = 0, a_2 = 2$
μ_3 :	$\frac{\alpha}{3}$	$\frac{2}{27}$	$a_0 = 0, a_1 = 1, a_2 = 0$
μ_4 :	$\frac{\alpha+\alpha^2}{3}$	$\frac{6}{27} = \frac{2}{9}$	$a_0 = 0, a_1 = 1, a_2 = 1$
μ_5 :	$\frac{\alpha+2\alpha^2}{3}$	$\frac{34}{27}$	$a_0 = 0, a_1 = 1, a_2 = 2$
μ_6 :	$\frac{2\alpha}{3}$	$\frac{16}{27}$	$a_0 = 0, a_1 = 2, a_2 = 0$
μ_7 :	$\frac{2\alpha+\alpha^2}{3}$	$\frac{20}{27}$	$a_0 = 0, a_1 = 2, a_2 = 1$
μ_8 :	$\frac{2\alpha+2\alpha^2}{3}$	$\frac{48}{27} = \frac{16}{9}$	$a_0 = 0, a_1 = 2, a_2 = 2$
μ_9 :	$\frac{1}{3}$	$\frac{1}{27}$	$a_0 = 1, a_1 = 0, a_2 = 0$
μ_{10} :	$\frac{1+\alpha^2}{3}$	$\frac{5}{27}$	$a_0 = 1, a_1 = 0, a_2 = 1$
μ_{11} :	$\frac{1+2\alpha^2}{3}$	$\frac{33}{27} = \frac{11}{9}$	$a_0 = 1, a_1 = 0, a_2 = 2$
μ_{12} :	$\frac{1+\alpha}{3}$	$\frac{3}{27} = \frac{1}{9}$	$a_0 = 1, a_1 = 1, a_2 = 0$
μ_{13} :	$\frac{1+\alpha+\alpha^2}{3}$	$\frac{1}{27}$	$a_0 = 1, a_1 = 1, a_2 = 1$
μ_{14} :	$\frac{1+\alpha+2\alpha^2}{3}$	$\frac{23}{27}$	$a_0 = 1, a_1 = 1, a_2 = 2$
μ_{15} :	$\frac{1+2\alpha}{3}$	$\frac{\frac{17}{4}}{27} = \frac{17}{108}$	$a_0 = 1, a_1 = 2, a_2 = 0$
μ_{16} :	$\frac{1+2\alpha+\alpha^2}{3}$	$\frac{9}{27} = \frac{1}{3}$	$a_0 = 1, a_1 = 2, a_2 = 1$
μ_{17} :	$\frac{1+2\alpha+2\alpha^2}{3}$	$\frac{25}{27}$	$a_0 = 1, a_1 = 2, a_2 = 2$
μ_{18} :	$\frac{2}{3}$	$\frac{8}{27}$	$a_0 = 2, a_1 = 0, a_2 = 0$
μ_{19} :	$\frac{2+\alpha^2}{3}$	$\frac{12}{27} = \frac{4}{9}$	$a_0 = 2, a_1 = 0, a_2 = 1$
μ_{20} :	$\frac{2+2\alpha^2}{3}$	$\frac{40}{27}$	$a_0 = 2, a_1 = 0, a_2 = 2$
μ_{21} :	$\frac{2+\alpha}{3}$	$\frac{10}{27}$	$a_0 = 2, a_1 = 1, a_2 = 0$
μ_{22} :	$\frac{2+\alpha+\alpha^2}{3}$	$\frac{2}{27}$	$a_0 = 2, a_1 = 1, a_2 = 1$
μ_{23} :	$\frac{2+\alpha+2\alpha^2}{3}$	$\frac{2}{27}$	$a_0 = 2, a_1 = 1, a_2 = 2$
μ_{24} :	$\frac{2+2\alpha}{3}$	$\frac{24}{27} = \frac{8}{9}$	$a_0 = 2, a_1 = 2, a_2 = 0$
μ_{25} :	$\frac{2+2\alpha+\alpha^2}{3}$	$\frac{4}{27}$	$a_0 = 2, a_1 = 2, a_2 = 1$
μ_{26} :	$\frac{2+2\alpha+2\alpha^2}{3}$	$\frac{8}{27}$	$a_0 = 2, a_1 = 2, a_2 = 2$

Aufgaben

Aufgaben 8

Aufgabe 51 (4=2+2 Punkte). Sei $K = \mathbb{Q}(\sqrt{7})$ und $L = \mathbb{Q}(\sqrt{17})$. Finde direkt (ohne Verwendung von Satz 2.4.15,), eine Ganzheitsbasis von $\mathfrak{o}_K$ und $\mathfrak{o}_L$. Bestimme die Diskriminante dieser Basis.

Aufgabe 52 (2 Punkt). Sei $K = \mathbb{Q}(w)$, mit $\mathfrak{m}_w = x^2 + x + 1$. Beschreibe $\mathfrak{o}_K$ und finde eine Ganzheitsbasis von K. Bestimme die Diskriminante dieser Basis.

Aufgabe 53 (3 Punkte). Sei $f(x) = x^3 + ax + b$ ein irreduzibles, normiertes kubisches Polynom und α eine Nullstelle.

i) (1 Teilpunkt) Was ist die Diskriminante von $\{1, \alpha, \alpha^2\}$?

ii) (2 Teilpunkte, je $0,5$ Punkte) Bestimme folgende Normen:

1. α
2. $\alpha - 3$
3. $1 + 2\alpha^2$
4. $1 - 2\alpha + 3\alpha^2$.

Aufgabe 54 (2 Punkte). Sei $K = \mathbb{Q}(\sqrt[3]{10})$.

i) (1 Teilpunkt) Beweise, dass

$$\{1, \sqrt[3]{10}, \sqrt[3]{100}\}$$

keine Ganzheitsbasis ist.

ii) (1 Teilpunkt) Gib einen Kandidaten für eine Ganzheitsbasis von $\mathfrak{o}_K$ und beschreibe wie man es auf Ganzheit überprüfen würde.

Aufgabe 55 (2 Punkte). Sei $K = \mathbb{Q}(\sqrt[4]{2})$ und

$$\mathcal{B} = \{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\}.$$

i) (1 Teilpunkt) Bestimme die Diskriminante von $\mathcal{B}$.

ii) (1 Teilpunkt) Beschreibe die Elemente, die man auf Ganzheit überprüfen, um zu zeigen, dass $\mathcal{B}$ eine Ganzheitsbasis ist?

Man darf für die folgende Aufgabe annehmen, dass ein Element $\alpha \in \mathfrak{o}_K$ genau dann invertierbar ist, wenn $\mathsf{N}(\alpha) = \pm 1$.

Aufgabe 56 (3 Punkte). Sei $d \in \mathbb{Z}$ quadratfrei und von $0,1$ verschieden. Ein Körper der Form $\mathbb{Q}(\sqrt{d})$ heißt reell-quadratisch wenn $d > 0$ und imaginär-quadratisch wenn $d < 0$.

i) (2 Teilpunkte) Beweise, dass die Einheiten $\mathfrak{o}_K^*$ von $\mathfrak{o}_K$ im imaginär-quadratischen Fall wie folgt sind:

$$\mathfrak{o}_K^* = \begin{cases} \{\pm 1, \pm i\}, & d = -1 \\ \{\pm 1, \pm \zeta_3, \pm \zeta_3^2\}, & d = -3 \\ \{\pm 1\} & \text{Ansonsten} \end{cases}$$

ii) (1=0.5+0.5 Teilpunkt) Sei $d = 2$.

ii a) Zeige, dass $a = 3 - 2\sqrt{2}$ eine Einheit ist in $\mathfrak{o}_K$, $K = \mathbb{Q}(\sqrt{d})$.

ii b) Beweise, dass die Einheiten $\mathfrak{o}_K^*$ eine unendliche Menge bilden.

2.4.4 Norm und Ganzheit in Eisenstein Körpern

Definition 2.4.22. Wir nennen einen Körper $\mathbb{Q}(\alpha)$ einen *Eisenstein* Körper falls das Minimalpolynom $\mathfrak{m}_\alpha$ von α das Eisenstein Kriterium erfüllt.

Bemerkung 2.4.23. Der Begriff *Eisenstein Körper* ist kein gängiger Begriff. Wir haben es eingeführt um die folgenden Aussagen sinngemäß zu ordnen.

Lemma 2.4.24. *Sei $\alpha \in \mathfrak{o}_K$ und erfülle $\mathfrak{m}_\alpha$ das Eisenstein Kriterium für die Primzahl p. Dann ist p ein Faktor von $\Delta(1, \alpha, \ldots, \alpha^{d-1})$.*

Beweis. Da $\mathfrak{m}_\alpha \in \mathbb{Z}[X]$ das Eisenstein Kriterium erfüllt und normiert ist (da $\alpha \in \mathfrak{o}_K$), haben wir

$$\mathfrak{m}_\alpha(x) = x^d \mod p$$

also

$$\mathfrak{m}'_\alpha(x) = dx^{d-1} \mod p.$$

In anderen Worten, es gibt ein $f(x) \in \mathbb{Z}[X]$, so dass

$$\mathfrak{m}'_\alpha(x) = dx^{d-1} + f(x)p.$$

Wir haben

$$\begin{aligned}
\mathsf{N}(\mathfrak{m}'_\alpha(\alpha)) &= \mathsf{N}(d\alpha^{d-1} + f(\alpha)p) \\
&= (d\alpha_1^{d-1} + f(\alpha)p)\cdots(d\alpha_d^{d-1} + f(\alpha)p) \\
&= d^d\alpha_1^{d-1}\cdots\alpha_d^{d-1} + p(\cdots) \\
&= d^d\alpha_1^{d-1}\cdots\alpha_d^{d-1} \mod p \\
&= \mathsf{N}(d\alpha^{d-1}) \mod p \\
&= \mathsf{N}(d)\mathsf{N}(\alpha)^{d-1} \mod p,
\end{aligned}$$

wobei $\alpha = \alpha_1, \ldots, \alpha_d$ die Konjugierten von α sind. Da α ganzalgebraisch ist, macht das modulo p Sinn für die Norm, da dies laut Proposition 2.3.14 in $\mathbb{Z}$ liegt. Von Korollar 2.2.10 ist es durch p teilbar (Eisenstein) und somit ist

$$\mathsf{N}(\alpha) = 0 \mod p \quad \Rightarrow \quad \mathsf{N}(\mathfrak{m}'_\alpha(\alpha)) = 0 \mod p.$$

Satz 2.2.24 besagt nun, dass

$$\Delta(1, \alpha, \ldots, \alpha^{d-1}) = 0 \mod p,$$

also durch p teilbar ist. □

Die nächste Aussage jedoch besagt, dass dieser p immer "unwichtig" sein wird wenn wir die Ganzheitsbasis berechnen wollen.

Proposition 2.4.25. *Sei $\alpha \in \mathfrak{o}_K$ und $K = \mathbb{Q}(\alpha)$ mit $[K : \mathbb{Q}] = d$. Wenn $\mathfrak{m}_\alpha$ das Eisenstein Kriterium für die Primzahl p erfüllt, dann ist*

$$\theta = \frac{1}{p}\sum_{i=0}^{d-1} a_i\alpha^i, \quad a_i \in \{0, \ldots, p-1\}$$

genau dann ganzalgebraisch, wenn $\theta = 0$.

Beweis. Beweis durch Widerspruch: Sei $\theta \in \mathfrak{o}_k$ und lass a_N das kleinste der $a_i \in \{0, \ldots, p-1\}$ sein, dass ungleich Null ist. Als solches haben wir

$$\theta = \frac{1}{p}\sum_{i=N}^{d-1} a_i\alpha^i \in \mathfrak{o}_K, \quad a_i \in \{0, \ldots, p-1\}.$$

Ausgeschrieben ist es

$$\begin{aligned}\theta &= \frac{1}{p}\left(a_N\alpha^N + a_{N+1}\alpha^{N+1} + a_{N+2}\alpha^{N+2} + \cdots + a_{d-1}\alpha^{d-1}\right)\\ &= \frac{1}{p}\left(a_N\alpha^N + \alpha^{N+1}\left(\underbrace{a_{N+1} + a_{N+2}\alpha + \cdots + a_{d-1}\alpha^{d-N-2}}_{\delta}\right)\right)\\ &= \frac{1}{p}\left(a_N\alpha^N + \alpha^{N+1}\delta\right), \quad \delta \in \mathfrak{o}_K.\end{aligned}$$

Wir multiplizieren beide Seiten mit α^{d-N-1} und erhalten

$$\alpha^{d-N-1}\theta = \frac{1}{p}\left(a_N\alpha^{d-1} + \alpha^d\delta\right) \in \mathfrak{o}_k.$$

Da α bei Annahme ganzalgebraisch war, ist $\mathfrak{m}_\alpha$ ein normiertes Polynom über $\mathbb{Z}$ vom Grad d (sieh Aussage der Proposition). Daher ist es von der Form

$$\mathfrak{m}_\alpha = b_0 + b_1x + \cdots + b_{d-1}x^{d-1} + x^d.$$

Von $\mathfrak{m}_\alpha(\alpha) = 0$ folgt nun

$$\alpha^d = p\left(\underbrace{-\left(\frac{b_{d-1}}{p}\alpha^{d-1} + \cdots + \frac{b_1}{p}\alpha + \frac{b_0}{p}\right)}_{g(\alpha)}\right).$$

Da $\mathfrak{m}_\alpha$ das Eisensteinkriterium erfüllt sind alle $\frac{b_j}{p} \in \mathbb{Z}$, daher gilt

$$\alpha^d = pg(\alpha), \quad g(x) \in \mathbb{Z}[X].$$

Da $\alpha \in \mathfrak{o}_K$ ganzalgebraisch ist, ist auch die polynomiale Kombination $g(\alpha) \in \mathfrak{o}_K$, auch wenn $g(x) \in \mathbb{Z}[X]$ nicht zwangsweise Normiert ist, solange die Koeffizienten in $\mathbb{Z}$ sind. Da auch $\theta, \delta \in \mathfrak{o}_K$d, ist

$$\frac{a_N\alpha^{d-1}}{p} = \alpha^{d-N-1}\theta - \frac{\alpha^d\delta}{p} = \alpha^{d-N-1}\theta - g(\alpha)\delta \in \mathfrak{o}_K.$$

Daher muss auch dessen Norm eine ganze Zahl sein. Dies wird gleich zum Widerspruch führen. Hierzu bemerke man, dass laut Eisenstein, b_0 nicht durch p^2 teilbar ist. Daher ist

$$\mathsf{N}(\alpha) = pr, r \in \mathbb{Z}$$

mit $p \nmid r$. Wir erhalten also

$$\begin{aligned}\mathsf{N}\left(\frac{a_N\alpha^{d-1}}{p}\right) &= \frac{\mathsf{N}(a_N)\mathsf{N}(\alpha)^{d-1}}{\mathsf{N}(p)}\\ &= \frac{a_N^d(pr)^{d-1}}{p^d}\\ &= \frac{a_N^d r^{d-1}}{p},\end{aligned}$$

was keine ganze Zahl sein kann, da $a_N \leq p-1$ bei Annahme ($a_i \in \{0, 1, \ldots, p-1\}$), also $p \nmid a_N$ und $p \nmid r$. □

2.4.5 Ganzheitsbasen von Kreisteilungskörper/Zyklotomische Körper

Definition 2.4.26. Sei $n \in \mathbb{Z}$. Ein Element $\zeta \in \mathbb{C}$ heißt die *n-te Einheitswurzel* wenn

$$\zeta^n = 1$$

gilt. Wenn es keinen $1 \leq r < n$ gibt, mit $\zeta^r = 1$, dann heißt ζ eine *primitive n-te Einheitswurzel*.

Manchmal werden wir ζ_n für die primitive n-te Einheitswurzel schreiben. Diese können bekanntlich auf dem Einheitskreis gedacht werden. Elemente des Einheitskreises werden multipliziert, indem man die Winkel (gegen dem Uhrzeigersinn) addiert. Als solches ist

$$\zeta_n = \exp\left(\frac{2\pi i}{n}\right)$$

immer eine n-te primitive Einheitswurzel.

Da diese immer die Gleichung

$$x^n - 1 = 0$$

erfüllen, sind Einheitswurzeln immer ganzalgebraisch. Diese Polynome sind allerdings nicht irreduzibel, vor allem bei $n = 2$ ist es sehr klar. Im allgemeinen haben wir

$$x^n - 1 = (x-1)(1 + x + x^2 + \cdots + x^{n-1}).$$

Die rechte Seite scheint irreduzibel zu sein, ist jedoch im allgemeinen auch nicht! Zum Beispiel haben wir

Beispiel 2.4.27.

$$1 + x + x^2 + x^3 = (1+x)(1+x^2).$$

Im Allgemeinen gilt allerdings

Proposition 2.4.28. *Das Polynom*

$$\mathfrak{m}_{\zeta_p} = 1 + x + x^2 + \cdots + x^{p-1}$$

ist genau dann irreduzibel, wenn $p \in \mathbb{N}$ prim ist.

Beweis. Aufgabe 30 besagt, dass $\mathfrak{m}_{\zeta_p}$ irreduzibel ist, wenn p prim ist.

Wenn $n = p$ nicht prim ist, dann gibt es $a, b \in \mathbb{N}$, so dass $ab = n$. Sei $y = x^a$. Wir haben

$$\begin{aligned} x^n - 1 = (x^a)^b - 1 &= (1 + y + y^2 + \cdots + y^{b-1})(y-1) \\ &= ((1 + x^a + (x^a)^2 + \cdots + (x^a)^{b-1}))(x^a - 1) \\ &= (1 + x^a + x^{2a} + \cdots + x^{ab-a})(1 + x + x^2 + \cdots + x^{a-1})(x-1). \end{aligned}$$

Auf der anderen Seite haben wir

$$x^n - 1 = (1 + x + x^2 + \cdots + x^{n-1})(x-1),$$

was zu

$$(1 + x^a + x^{2a} + \cdots + x^{ab-a})(1 + x + x^2 + \cdots + x^{a-1}) = (1 + x + x^2 + \cdots + x^{n-1})$$

führt. □

Definition 2.4.29. Körper der Form $\mathbb{Q}(\zeta_p)$ werden *zyklotomische* bzw. *Kreisteilungskörper* genant, wenn p eine Primzahl und ζ_p ein primitives p-tes Einheitswurzel ist.

In anderen Worten, wenn das Minimalpolynom von ζ_p das Polynom $1 + x + \cdots + x^{p-1}$ ist.

Lemma 2.4.30. *Sei $\mathbb{Q}(\zeta_p)$ ein Kreisteilungskörper. Dann gilt*

i) $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$,

ii) $\mathsf{N}(\zeta) = 1$,

iii) $\mathsf{N}(\zeta - 1) = p$.

Beweis. i) Der Grad von $\mathfrak{m}_{\zeta_p}$ ist klar $p-1$. Lemma 1.3.28 impliziert nun das Resultat.

ii) Lemma 2.2.10 mithilfe des Minimalpolynoms $\mathfrak{m}_{\zeta_p}$.

iii) Das Gleiche wie *ii*), nur für das Minimalpolynom $\mathfrak{m}_{\zeta_p - 1}$. Hierzu sehe man sich den Beweis von Proposition 2.4.28 an.

□

Satz 2.4.31. *Sei $\mathbb{Q}(\zeta_p)$ ein Kreisteilungskörper. Dann ist*

$$\mathcal{Z} = \{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$$

eine Ganzheitsbasis und

$$\Delta(\mathcal{Z}) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}.$$

In anderen Worten

$$\mathfrak{o}_K = \mathbb{Z}[\zeta].$$

Beweis. Satz 2.2.24 besagt, dass

$$\Delta(\mathcal{Z}) = (-1)^{\frac{(p-1)(p-2)}{2}} \mathsf{N}(\mathfrak{m}'_\zeta(\zeta)).$$

Da $\mathfrak{m}_{\zeta_p}(x) = \frac{x^p - 1}{x-1}$ folgt

$$\mathfrak{m}'_{\zeta_p}(x) = \frac{px^{p-1}(x-1) - (x^p - 1)}{(x-1)^2}.$$

Daher ist

$$\begin{aligned} \mathfrak{m}'_{\zeta_p}(\zeta) &= \frac{p\zeta^{p-1}(\zeta - 1) - (\zeta^p - 1)}{(\zeta - 1)^2} \\ &= \frac{p\zeta^{p-1}}{\zeta - 1} - \frac{\zeta^p - 1}{\zeta - 1} \cdot \frac{1}{\zeta - 1} \\ &= \frac{p\zeta^{p-1}}{\zeta - 1} \end{aligned}$$

da $\frac{\zeta^p - 1}{\zeta - 1} = \mathfrak{m}_\zeta = 0$. Die Multiplikativität der Norm (Proposition 2.2.6) ergibt nun

$$\begin{aligned} \mathsf{N}(\mathfrak{m}'_\zeta(\zeta)) &= \mathsf{N}\left(\frac{p\zeta^{p-1}}{\zeta - 1}\right) \\ &= \frac{\mathsf{N}(p)\mathsf{N}(\zeta)^{p-1}}{\mathsf{N}(\zeta - 1)} \\ &= \frac{p^{p-1} \cdot 1^{p-1}}{p} \\ &= p^{p-2}. \end{aligned}$$

Hier haben wir Lemmas 2.2.8 und 2.4.30 benutzt. Daraus folgt, dass

$$\Delta(\mathcal{Z}) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}.$$

Sei $\mathcal{Z}' = \{1, (\zeta - 1), (\zeta - 1)^, \ldots, (\zeta - 1)^{p-2}\}$. Laut Korollar 2.2.25 haben wir

$$\Delta(\mathcal{Z}') = \Delta(\mathcal{Z}),$$

wessen einziger Teiler p ist. Schritt 4 unseres Algorithms im Abschnitt 2.4.1 besagt, dass die einzigen Elemente, die wir auf Ganzalgebraität überprüfen brauchen von der Form

$$\sum_{i=0}^{p-2} \frac{1}{p} a_i (\zeta - 1)^i \quad a_i \in \{0, \ldots, p-1\}$$

sind. Proposition 2.4.25 besagt nun, dass diese nie ganzalgebraisch sind, da das Minimalpolynom $\mathfrak{m}_{\zeta-1}$ das Eisenstein Kriterium für p erfüllt. Daher ist $\mathcal{Z}'$ eine Ganzheitsbasis uns als solches ist auch $\mathcal{Z}$ eine Ganzheitsbasis, da beide in $\mathbb{Z}$ liegen und die gleiche Diskriminante haben, siehe Satz 2.4.4. □

Aufgaben

Aufgaben 9

Aufgabe 57 (2 Punkte). Sei α ein algebraisches Element und $\mathfrak{m}_\alpha = x^a - a^k$, wobei $a \in \mathbb{Z}$ und $k \in \mathbb{N}$. Beweise mithilfe des Eisensteinkriteriums, dass

$$\mathcal{B} = \{1, \alpha, \dots, \alpha^{a-1}\}$$

eine Ganzheitsbasis ist.

Aufgabe 58 (6 Punkte). Sei

$$\zeta_n = \exp\left(\frac{2\pi i}{n}\right).$$

Für einen beliebigen $n \geq 1$ definieren wir das n-te zyklotomische Polynom $\Phi_n(x)$ durch Induktion, wobei

$$\Phi_1(x) = x - 1$$
$$\vdots$$
$$\Phi_n(x) = \frac{x^n - 1}{\prod \Phi_d(x)}.$$

Das Produkt wird hier über alle Teiler von n genommen, also $d \mid n$. Daher gilt

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

i) Beweise, dass
$$\Phi_n(\zeta_n) = 0.$$

ii) Sei $n = p$ eine Primzahl. Beweise, dass

$$\Phi_p(x) = 1 + x + \cdots + x^{p-1}.$$

Von nun an, sei $n = p^k$, wobei p eine Primzahl ist und $k \geq 2$.

iii) Zeige, dass
$$\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}}) = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}}.$$
Spezifisch, dass $\mathsf{grad}(\Phi_{p^k}(x)) = p^k - p^{k-1}$.

iv) Beweise, dass $\Phi_{p^k}(x+1)$ das Eisensteinkriterium erfüllt und als solches irreduzibel ist. Schlussfolgere, dass ür $n = p^k$, Φ_n das Minimalpolynom von ζ_n ist und daher
$$[\mathbb{Q}(\zeta_{p^k}) : \mathbb{Q}] = p^k - p^{k-1}$$
gilt. (Es wurde schon von Gauß beweisen, dass Φ_n für alle n irreduzibel ist!)

v) Beweise, dass, bis au Vorzeichen, $\Delta(1, \zeta_n, \cdots, \zeta_n^m)$ ein Vielfaches von p ist. Hier gilt $n = p^k$ und $m = p^k - p^{k-1}$.

vi) Sei $K = \mathbb{Q}(\zeta_{p^k})$. Schlussfolgere, dass $\mathfrak{o}_K = \mathbb{Z}[\zeta_{p^k}]$.

Wem es zu allgemein ist, kann Aufgaben iii)-vi) auch nur für die Fälle $n = 8$ und $n = 9$ beweisen.

3 Faktorisierung in $\mathfrak{o}_K$

Wir wollen nun die Faktorisierung von Elementen in $\mathfrak{o}_K$ studieren. Dafür müssen wir aber erst einiges über Einheiten und Irreduzibilität lernen, da Faktorisierung ja bedeutet, dass wir etwas als Produkt von einer Einheit und irreduziblen Elementen zerlegen.

Lemma 3.0.1. *Sei K ein Zahlenkörper, $0 \neq \alpha \in K$ und $\alpha = \sigma_1(\alpha), \ldots, \sigma_d(\alpha)$ die Konjugierten von α. Dann ist*

$$\prod_{i=2}^{d} \sigma_i(\alpha) \in K.$$

Des weiteren, wenn $\alpha \in \mathfrak{o}_K$ ganzalgebraisch ist, folgt

$$\prod_{i=2}^{d} \sigma_i(\alpha) \in \mathfrak{o}_K.$$

Spezifisch gilt $\alpha \mid \mathsf{N}(\alpha)$ in $\mathfrak{o}_K$.

Beweis. Der erste Teil ist die Definition der Norm, da $\mathsf{N}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha) \in \mathbb{Q} \subseteq K$ und somit folgt aus $0 \neq \alpha = \sigma_1(\alpha) \in K$, dass $\prod_{i=2}^{d} \sigma_i(\alpha) = \frac{\prod_{i=1}^{d} \sigma_i(\alpha)}{\alpha} \in K$.

Für den zweiten Teil bemerken wir, dass $\mathfrak{o}_K = \mathfrak{o}_{\hat{\mathbb{Q}}} \cap K$, wobei $\hat{\mathbb{Q}}$ die algebraische Abschließung von $\mathbb{Q}$ ist. Das heißt, $\mathfrak{o}_{\hat{\mathbb{Q}}}$ besteht aus der Menge aller α's, so dass es ein ganzzahliges Polynom $f(x) \in \mathbb{Z}[X]$ gibt, mit $f(\alpha) = 0$.

Sei $\prod_{i=2}^{d} \sigma_i(\alpha) \in \mathfrak{o}_{\hat{\mathbb{Q}}}$, was ganzalgebraisch ist, denn es ist nach Korollar 2.3.4 das Produkt von ganzalgebraischen Elementen. Um zu schlussfolgern, dass es auch in $\mathfrak{o}_K$ liegt, benutzen wir unsere Bemerkung, dass $\mathfrak{o}_K = \mathfrak{o}_{\hat{\mathbb{Q}}} \cap K$ und den ersten Teil dieses Lemmas. Die Definition der Norm

$$\mathsf{N}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha) = \alpha \times \prod_{i=2}^{d} \sigma_i(\alpha)$$

impliziert nun auch, dass α seine Norm in $\mathfrak{o}_K$ teilt. □

Man erinnere sich an die Definition 1.3.9 von irreduziblen, reduziblen und invertierbaren Elementen.

Proposition 3.0.2. *Eine ganzalgebraische Zahl $\alpha \in \mathfrak{o}_K$ ist genau dann invertierbar, wenn*

$$\mathsf{N}(\alpha) = \pm 1.$$

Beweis. Sei α invertierbar in $\mathfrak{o}_K$. Also, es gibt ein $\alpha^{-1} \in \mathfrak{o}_K$, so dass $\alpha\alpha^{-1} = 1$. Aus Proposition 2.2.6 folgt, dass

$$\mathsf{N}(\alpha)\mathsf{N}(\alpha^{-1}) = \mathsf{N}(\alpha\alpha^{-1}) = \mathsf{N}(1) = 1.$$

Da aus Proposition 2.3.14 folgt, dass $\mathsf{N}(\alpha), \mathsf{N}(\alpha^{-1}) \in \mathbb{Z}$, muss $\mathsf{N}(\alpha) = \pm 1$ sein.

Auf der anderen Seite, sei $\mathsf{N}(\alpha) = \pm 1$. Proposition 2.2.5 sagt aus, dass $\alpha \neq 0$. Wir können also Lemma 3.0.1 anwenden und schlussfolgern, dass $\alpha \mid \mathsf{N}(\alpha) = \pm 1$ in $\mathfrak{o}_K$. Dies jedoch bedeutet genau, dass α in $\mathfrak{o}_K$ invertierbar ist. Das Inverse (wie in Lemma 3.0.1 besprochen) ist $\prod_{i=2}^{d} \sigma_i(\alpha)$. □

Korollar 3.0.3. *Sei K ein Zahlenkörper, $I \subseteq \mathfrak{o}_K$ ein Ideal und $\alpha \in I$. Dann ist*

$$\mathsf{N}(\alpha) \in I.$$

Beweis. Laut Lemma 3.0.1 gilt $\alpha \mid \mathsf{N}(\alpha)$, was $\mathsf{N}(\alpha) \in (\alpha) \subseteq I$ impliziert. □

Proposition 3.0.4. *Sei $\alpha \in \mathfrak{o}_K$ mit $\mathsf{N}(\alpha) = p$, eine Primzahl. Dann ist α irreduzibel in $\mathfrak{o}_K$.*

Beweis. Sei $\alpha = \beta\gamma$, mit $\beta, \gamma \in \mathfrak{o}_K$. Durch Proposition 2.2.6 habe wir

$$\mathsf{N}(\alpha) = p = \mathsf{N}(\beta)\mathsf{N}(\gamma).$$

Aus p, prim folgt, o. B. d. A., dass $\mathsf{N}(\beta) = 1$. Proposition 3.0.2 impliziert die Invertierbarkeit von β woraus wir die Irreduzierbarkeit von α schließen können. □

Bemerkung 3.0.5. Die Umkehrung der Aussage ist *nicht* richtig!

Beispiel 3.0.6. Sei $3 \in \mathbb{Z}[i]$. Es hat Norm $\mathsf{N}(3) = 9$. Für einen allgemeinen Element gilt

$$\mathsf{N}(x + iy) = x^2 + y^2,$$

was nie ± 3 über $\mathbb{Z}$ werden kann. Es gibt also kein Element in $\mathbb{Z}[i]$ mit Norm 3 und wir schließen, dass $3 \in \mathbb{Z}[i]$ irreduzibel ist.

Bemerkung 3.0.7. Auch muss die Norm nicht zwingend die Potenz einer Primzahl sein!

Beispiel 3.0.8. Das Element $1 + \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ ist irreduzibel. Es gilt

$$\mathsf{N}(1 + \sqrt{-5}) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 1 + 5 = 6 = 2 \cdot 3.$$

Da jedes Element von der Form $a + b\sqrt{-5}$ ist, haben wir

$$\mathsf{N}(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Es ist klar, dass weder 2 noch 3 von dieser Form sind.

Satz 3.0.9. *Sei $\alpha \in \mathfrak{o}_K \setminus \{0\}$. Es gibt eine Einheit $\upsilon \in \mathfrak{o}_K^\times$ und irreduzible Elemente $\pi_1, \ldots, \pi_n$, so dass*

$$\alpha = \upsilon\pi_1 \cdots \pi_n.$$

Beweis. Wir beweisen es durch Induktion auf dem Betrag der Norm. Für $|\mathsf{N}(\alpha)| = 1$ folgt es durch Proposition 3.0.2. Wir nehmen an, dass es für alle $\beta \in \mathfrak{o}_K$ stimmt, mit $|\mathsf{N}(\beta)| < n$. Sei $|\mathsf{N}(\alpha)| = n$. Wenn α irreduzibel ist, hat es sich erledigt. Andernfalls gibt es $\beta, \gamma \in \mathfrak{o}_K$, mit $1 < |\mathsf{N}(\beta)|, |\mathsf{N}(\gamma)| < n$, so dass $\alpha = \beta\gamma$. Da der Betrag der Norm von β und γ kleiner als n ist, können wir es, laut Induktionsannahme, in irreduzible Komponente zerteilen. □

Diese Aussage hält für allgemeine Noetherische Ringe. Der Beweis ist auch nicht viel schwerer. Wir zerteilen ein Element immer weiter in kleinere Teile. Die Hauptideale bilden dann eine aufsteigende Kette, welches, bei Definition eines Noetherischen Ringes, stabilisieren muss. Wir belassen es aber bei unserem obigen Argument, da wir nicht mehr brauchen werden.

Definition 3.0.10. Ein Ring heißt *faktoriell* (oder manchmal auch *Gaußscher Ring*) wenn für alle irreduzible Elemente $\pi_1, \ldots, \pi_r, \tau_1, \ldots, \tau_s \in \mathfrak{o}_K$, aus

$$\pi_1 \cdots \pi_r = \tau_1 \cdots \tau_s$$

folgt, $r = s$ und nach Neuordnung, $\pi_i = \upsilon_i\tau_i$, $1 \le i \le r = s$. Die $\upsilon_i \in \mathfrak{o}_K^\times$ sind invertierbare Elemente.

Wohlbekannte Beispiele von faktoriellen Ringen sind Körper, $\mathbb{Z}$ und $R[X]$, wo R selber ein faktorielles Ring ist. Für einen Beispiel eines Ringes wo dies nicht hält, sieh folgendes:

Beispiel 3.0.11. Sei $K = \mathbb{Q}(\sqrt{-10})$. Dann ist $\mathfrak{o}_K = \mathbb{Z}[\sqrt{-10}]$ und es gilt

$$10 = 2 \times 5 = -(\sqrt{-10}) \times \sqrt{-10}.$$

Zu sehen, dass $2, 5$ und $\sqrt{-10}$ alle irreduzibel in $\mathfrak{o}_K$ sind betrachten wir deren Norm. Wir haben

$$\mathsf{N}(2) = 4 = 2 \times 2, \quad \mathsf{N}(5) = 25 = 5 \times 5 \quad \text{und} \quad \mathsf{N}(\sqrt{-10}) = 10 = 2 \times 5.$$

Es bleibt zu zeigen, dass es keinen Element α in $\mathbb{Z}[\sqrt{-10}]$ gibt, dessen Norm ± 2 oder ± 5 ist. Dafür, betrachte die allgemeine Form $\alpha = x + \sqrt{-10}y$ eines Elements in $\mathbb{Z}[\sqrt{-10}]$. Wir haben

$$\mathsf{N}(\alpha) = \mathsf{N}(x + \sqrt{-10}y) = x^2 + 10y^2, \quad \text{mit} \quad x, y \in \mathbb{Z}.$$

Es ist leicht zu sehen, dass die Gleichungen $x^2 + 10y^2 = \pm 2$ und $x^2 + 10y^2 = \pm 5$ über $\mathbb{Z}$ keine Lösung haben.

Bemerkung 3.0.12. Im obigen Beispiel haben wir die Tatsache benutzt, dass -10 nicht irreduzibel über $\mathbb{Z}$ ist um das ganze etwas einfacher zu machen. Eine natürliche Frage ist, ob man auch eine Primzahl $p \in \mathbb{Z}$ finden kann, so dass $\mathbb{Z}[\sqrt{p}]$ kein faktorielles Ring ist. Die Antwort ist ja, die kleinste Primzahl bei denen es so ist, ist jedoch 79.

Die andere Annahme, die man machen könnte, dass $\mathbb{Z}[n]$ nie faktoriell ist, wenn n nicht prim oder 1 ist, wäre auch nicht richtig. Zum Beispiel ist $\mathbb{Z}[\sqrt{6}]$ faktoriell. Wir haben jetzt noch nicht genug Methoden um dies einfach zu beweisen, aber als Indiz sagen wir, dass die Norm eines allgemeinen Elements $x + \sqrt{6}y \in \mathbb{Z}[\sqrt{6}]$ gleich $x^2 - 6y^2$ ist. Daher gibt es Elemente mit Norm 3.

Eine Möglichkeit um mit diesem neuen Problem umzugehen, ist Ideale einzuführen.

3.1 Eindeutige faktorisierung von Idealen

Wie in Bemerkung 1.1.17 erwähnt ist das Produkt $I \times J := (ij \mid i \in I, j \in J)$ von Idealen $I, J \in R$ wieder ein Ideal von R. Bei Hauptidealen gilt

$$(x)(y) = (xy),$$

wobei wir $(x)(y)$ für $(x) \times (y)$ schreiben. Allgemeiner gilt

$$(x, y)(z, w) = (xz, xw, yz, yw).$$

Beispiel 3.1.1. Lass uns zum Beispiel 3.0.11 zurückkehren. Betrachte die Ideale

$$\mathfrak{p} := (2, \sqrt{-10}), \quad \mathfrak{q} := (5, \sqrt{-10}).$$

Es gilt

$$\begin{aligned}
\mathfrak{pq} &= (2, \sqrt{-10})(5, \sqrt{-10}) \\
&= (10, 2\sqrt{-10}, 5\sqrt{-10}, -10) \\
&= (10, 2\sqrt{-10}, 5\sqrt{-10}, -10, \sqrt{-10}) && \text{da } \sqrt{-10} = 5\sqrt{-10} - 2 \cdot 2\sqrt{-10} \\
&= (\sqrt{-10}) \\
\mathfrak{p}^2 &= (2, \sqrt{-10})(2, \sqrt{-10}) \\
&= (4, 2\sqrt{-10}, -10) \\
&= (4, 2\sqrt{-10}, -10, 2) && \text{da } 2 = -(-10 + 2 \cdot 4) \\
&= (2) \\
\mathfrak{q}^2 &= (5, \sqrt{-10})(5, \sqrt{-10}) \\
&= (25, 5\sqrt{-10}, -10) \\
&= (25, 5\sqrt{-10}, -10, 5) && \text{da } 5 = 25 + 2 \cdot (-10) \\
&= (5).
\end{aligned}$$

Daher folgt, dass

$$(10) = (2)(5) = \mathfrak{p}^2\mathfrak{q}^2 \qquad \text{und} \qquad (10) = (\sqrt{-10})^2 = (pq)^2.$$

Als ein Element hat $10 \in \mathbb{Z}[\sqrt{-10}]$ zwei verschiedene Faktorisierung in irreduzible Elemente. Als Hauptideale aufgefasst sind diese Elemente/Ideale aber weiter zerlegbar und stimmen danach miteinander überein.

Wir wollen verstehen, was hier passiert ist und wie weit man so was als Satz formulieren kann. Ein Großteil des verbleibenden Kurses wird sich mit dieser Frage beschäftigen.

Einige auffällige Sachen, die man hier schon sehen kann sind die Tatsache, dass $\mathfrak{p}$ und $\mathfrak{q}$ Primideale (sogar Maximalideale) sind und dass Hauptideale eine große Rolle spielen. Des weiteren bemerken wir, dass wir Ideale haben, die keine Hauptideale sind, z. B., $\mathfrak{p}$ und $\mathfrak{q}$. Daher ist $\mathbb{Z}[\sqrt{-10}]$ kein Hauptidealring.

Proposition 3.1.2. *Sei $R \neq \{0\}$ ein endlicher Integritätsbereich. Dann ist R ein Körper.*

Beweis. Sei $r \in R \setminus \{0\}$ und betrachte $r, r^2, \ldots$. Da R endlich ist können nicht alle r^i verschieden sein. In anderen Worten, es gibt $i > j \in \mathbb{N}$, so dass

$$r^i = r^j.$$

Wir haben

$$r^j(r^a - 1) = 0, \quad \text{wobei } a = i - j \geq 1.$$

Da $r \neq 0$ und R ein Integritätsbereich ist, folgt, dass $r^j \neq 0$ und als solches, $x^a - 1 = 0$. Dies impliziert $x^a = 1$ woraus $xx^{a-1} = 1$ folgt. Also ist x invertierbar. □

3.2 Noetherheit von $\mathfrak{o}_K$

Lemma 3.2.1. *Sein $I \subseteq J \subseteq R$ Ideale eines Ringes R, so dass R/I endlich ist. Es gilt*

$$|R/I| \geq |R/J|,$$

mit Gleichheit genau dann, wenn $I = J$.

Beweis. Dies ist einfach nur der zweite Isomorphiesatz 1.1.47 welches besagt, dass

$$R/J \simeq (R/I)/(J/I).$$

Da wir R/I weiter teilen, kann es nur kleiner werden. Des weiteren wird es genau dann gleich groß bleiben, wenn J/I das Nullideal in R/I ist, was in R zu I korrespondiert. In anderen Worten, wenn $J = I$. □

Proposition 3.2.2. *Sei $\{0\} \neq I \subseteq \mathfrak{o}_K$ ein nicht-triviales Ideal. Dann ist $\mathfrak{o}_K/I$ endlich.*

Beweis. Sei $0 \neq \alpha \in I$. Laut Korollar 3.0.3 ist $n := \mathsf{N}(\alpha) \in I$, woraus $(n) \subseteq I$ folgt. Aufgrund von Lemma 3.2.1 bleibt es zu zeigen, dass $\mathfrak{o}_K/(n)$ endlich ist.

Die zugrundeliegende Abelsche Gruppe eines Quotienten von einem Ring mit einem Ideal ist das Quotient der zugrundeliegenden Abelschen Gruppe[1]. Als Abelsche Gruppe ist $\mathfrak{o}_K \simeq \mathbb{Z}^k, k \in \mathbb{N}$, laut Korollar2.4.5. Es gilt daher

$$\#(\mathfrak{o}_K/(n)) = \#(\mathfrak{o}_K/n\mathfrak{o}_K) = \#\left(\mathbb{Z}^k/n\mathbb{Z}^k\right) = n^k.$$

□

Bemerkung 3.2.3. Als Abelsche Gruppen setzen wir *nicht* das Element $(n, 0, \ldots, 0) \in \mathbb{Z}^k$ gleich Null, sondern das Element $(n, n, \ldots, n) \in \mathbb{Z}^k$.

Korollar 3.2.4. *Jedes nicht-triviale Primideal $\{0\} \neq \mathfrak{p} \subseteq \mathfrak{o}_K$ ist maximal.*

Beweis. Dies ist eine Zusammenführung von Propositionen 1.1.49, 3.1.2 und 3.2.2. Genauer:

$$\mathfrak{p} \neq \{0\} = = \overset{3.2.2}{=} \Rightarrow \mathfrak{o}_K/\mathfrak{p} = \text{endlich} \overset{3.1.2}{= = = = = = = = = = \Rightarrow} \mathfrak{o}_K/\mathfrak{p} = \text{Körper} \overset{1.1.49}{= =} \Rightarrow \mathfrak{p} = \text{maximal.}$$

$$\mathfrak{p} = \text{prim} \overset{1.1.49}{= =} \Rightarrow \mathfrak{o}_K/\mathfrak{p} = \text{Integritätsbr.} \overset{}{= = = = = = = = = = \Rightarrow}$$

□

[1] Zur Erläuterung: Hierzu erinnere man sich an die Konstruktion eines Quotienten von einem Ring mit einen Ideal. Wir habe das Quotient genauso gemacht wie man mit Untergruppen teilt und die Restklassengruppe mit einer Ringstruktur versehen. Das ist, was wir mit dem obigen Satz meinen. Man kann es auch etwas anders ausdrücken und sagen, "das Quotient ist mit dem Vergessensfunktor verträglich".

Proposition 3.2.2 erlaubt uns folgende Definition einzuführen:

Definition 3.2.5. Sei $I \neq 0$ ein nicht-triviales Ideal von $\mathfrak{o}_K$. Wir definieren die *Norm eines Ideals* als

$$\mathsf{N}(I) := |\mathfrak{o}_K/I|,$$

wobei $|\mathfrak{o}_K/I|$ die Anzahl der Elemente in $\mathfrak{o}_K/I$ bezeichnet.

Definition 3.2.6. Ein Ring R heißt *Noethersch* wenn es die *aufsteigende Kettenbedingung* erfüllt: Das heißt, wenn für jede aufsteigende Folge von Idealen

$$I_1 \subseteq I_2 \subseteq \cdots$$

von R, es einen $N \in \mathbb{N}$ gibt, so dass

$$I_N = I_{N+1} = I_{N+2} = \cdots.$$

Proposition 3.2.7. *Ein algebraischer Zahlenring $\mathfrak{o}_K$ ist Noethersch.*

Beweis. Sei

$$I_1 \subseteq I_2 \subseteq \cdots$$

gegeben. Laut Lemma 3.2.1 erhalten wir eine absteigende Sequenz

$$\mathsf{N}(I_1) \geq \mathsf{N}(I_2) \geq \cdots,$$

mit Gleichung $\mathsf{N}(I_i) = \mathsf{N}(I_{i+1})$ genau dann, wenn $I_i = I_{i+1}$, was aufgrund der Endlichkeit von $\mathsf{N}(I_1)$ (Proposition 3.2.2) stabilisieren muss. □

Diese folgende Aussage ist der erste Teil einer stärkeren Aussage, die wir bald beweisen werden:

Lemma 3.2.8. *Sei $\{0\} \neq I \subseteq \mathfrak{o}_K$ ein nicht-triviales Ideal. Es gibt Maximalideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, so dass*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq I.$$

Beweis. Beweis durch "umgekehrte" Induktion. Also, nehmen an, dass es für alle Ideale J echt größer als I stimmt, und beweisen es dann für I. Induktionsanfang ist hier ein Maximalideal $J = \mathfrak{p}$, da es für Maximalideale bei tautologisch stimmt.

Sei I nun kein Maximalideal, daher, laut Korollar 3.2.4, ist es auch nicht prim. Es gibt also Ideale A, B, so dass $AB \subseteq I$, aber $A \notin I$ und $B \notin I$ (Lemma 1.1.34).

Sei $A' := (A, I)$, das Ideal erzeugt mit A und I (also, der Schnitt aller Ideale, die sowohl A, wie auch I enthalten) und $B' = (B, I)$. Es gilt $A'B' = (A, I)(B, I) = (AB, AI, BI, I^2) \subseteq (I)$, da jedes der erzeugenden Ideale in I liegt. Es gilt auch, dass $A' \notin I$ und $B' \notin I$.

Da jedoch $A' = (A, I), B' = (B, I) \supsetneq I$ echt größer sind (da $A \notin I, B \notin I$), gibt es Maximalideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ und $\mathfrak{b}_1, \ldots, \mathfrak{b}_s$, so dass

$$\mathfrak{a}_1 \cdots \mathfrak{a}_r \subseteq A' \quad \text{und} \quad \mathfrak{b}_1 \cdots \mathfrak{b}_s \subseteq B'.$$

Daher

$$\mathfrak{a}_1 \cdots \mathfrak{a}_r \mathfrak{b}_1 \cdots \mathfrak{b}_s \subseteq A'B' \subseteq I,$$

was unser Induktionsschritt ist. □

Aufgaben

Aufgaben 10

Aufgabe 59 (4 Punkte). Sei $K = \mathbb{Q}(\sqrt{-6})$ und betrachte $\mathfrak{o}_K$. Es gilt

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}).$$

i) (1 Teilpunkt) Zeige, dass es in $\mathfrak{o}_K$ keinen Element der Norm 2 oder 5 gibt und schlussfolgere, dass es zwei echt verschiedene Faktorisierungen von $10 \in \mathfrak{o}_K$ in irreduziblen Elemente gibt.

ii) (2 Teilpunkte) Beweise, dass $\mathfrak{a} = (2, \sqrt{-6})$ ein Maximalideal von $\mathfrak{o}_K$ ist. Ferner, zeige, dass $\mathfrak{a}$ kein Hauptideal ist.

iii) (1 Teilpunkt) Zeige, dass $\mathfrak{a}^2 = (2)$.

Aufgabe 60 (6 Punkte). Sei $K = \mathbb{Q}(\sqrt{-5})$ und $\mathfrak{o}_K$ dessen assoziiertes Zahlenring.

i) (1 Teilpunkt) Zeige, dass $2\mathfrak{o}_K = \mathfrak{p}_2^2$, wobei

$$\mathfrak{p}_2 = (2, 1 + \sqrt{-5}).$$

Bestimme die Norm von $\mathfrak{p}_2$.

ii) (1 Teilpunk) Zeige, dass $3\mathfrak{o}_K = \mathfrak{p}_3\mathfrak{q}_3$, wobei

$$\mathfrak{p}_3 = (3, 1 + \sqrt{-5})$$

und

$$\mathfrak{q}_3 = (3, 1 - \sqrt{-5}).$$

iii) (1 Teilpunkt) Zeige, dass $5\mathfrak{o}_K = \mathfrak{p}_5^2$, wobei

$$\mathfrak{p}_5 = (\sqrt{-5}).$$

iv) (1 Teilpunkt) Zeige, dass $7\mathfrak{o}_K = \mathfrak{p}_7\mathfrak{q}_7$, wobei

$$\mathfrak{p}_7 = (7, 3 + \sqrt{-5})$$

und

$$\mathfrak{q}_7 = (7, 3 - \sqrt{-5}).$$

v) (2 Teilpunkte) Betrachte die Ideale $\mathfrak{p}_3$ und $\mathfrak{q}_3$. Zeige, dass jedes Element $a + b\sqrt{-5} \in \mathfrak{q}_3$ die Eigenschaft hat, dass $a + b$ durch 3 teilbar ist, also $3 \mid a + b$ gilt.

Gleichwie, dass jedes Element $c + d\sqrt{-5} \in \mathfrak{p}_3$ die Eigenschaft hat, dass $c - d$ ein Vielfaches von 3 ist.

vi) Zeige, dass $\mathfrak{p}_3$ und $\mathfrak{q}_3$ keine Hauptideale sind.

Aufgabe 61 (6 Punkte). Sei $K = \mathbb{Q}(\sqrt{d})$.

i) (1 Teilpunkt) Sei $d \equiv 2 \mod 4$. Zeige, dass

$$2\mathfrak{o}_K = \left(2, \sqrt{d}\right)^2$$

und das $\mathfrak{p} = \left(2, \sqrt{d}\right)$ ein Maximalideal ist.

ii) (1 Teilpunkt) Sei $d \equiv 3 \mod 4$. Zeige, dass

$$2\mathfrak{o}_K = \left(2, 1+\sqrt{d}\right)^2$$

und das $\mathfrak{p} = \left(2, 1+\sqrt{d}\right)$ ein Maximalideal ist.

iii) (2 Teilpunkte) Sei $d \equiv 1 \mod 8$. Zeige, dass

$$2\mathfrak{o}_K = \mathfrak{p}\mathfrak{q},$$

wobei $\mathfrak{p} = \left(2, \frac{1+\sqrt{d}}{2}\right)$ und $\mathfrak{q} = \left(2, \frac{1-\sqrt{d}}{2}\right)$. Des weiteren, zeige, dass $\mathfrak{p}, \mathfrak{q}$ unterschiedliche Maximalideale sind.

iv) (2 Teilpunkte) Sei $d \equiv 5 \mod 8$. Zeige, dass $2\mathfrak{o}_K$ ein Maximalideal ist.

Aufgabe 62 (5 Punkte). Sei $\alpha = \sqrt[3]{2}$ und $K = \mathbb{Q}(\alpha)$. Dann ist $\mathfrak{o}_K = \mathbb{Z}[\alpha]$ mit Ganzheitsbasis $\{1, \alpha, \alpha^2\}$. Wir definieren $\mathfrak{p} = (5, 2+\alpha)$ und $\mathfrak{q} = (5, 4+3\alpha+\alpha^2)$.

i) (2 Teilpunkte) Beweise, dass das Polynom x^2+3x+4 irreduzibel ist über $\mathbb{F}_5$ und schlussfolgere, dass $\mathfrak{q}$ ein Maximalideal von $\mathfrak{o}_K$ ist. Man darf annehmen, dass irreduzible Elemente von $\mathbb{F}_5[X]$ zu Maximalideale korrespondieren. (*Tipp: Was kann man über den Kern einer surjektiven Abbildung in einem Körper sagen?*)

ii) (2 Teilpunkte) Zeige, dass es einen wohldefinierten Ringhomomorphismus

$$\mathfrak{o}_K \to \mathbb{F}_5$$

gibt, mit $f(\alpha) = 3 \in \mathbb{F}_5$. Schlussfolgere, dass $\mathsf{Ker}(f) = \mathfrak{p}$ ein Maximalideal von $\mathfrak{o}_K$ ist.

iii) (1 Teilpunkt) Bestätige, dass

$$1 = 5 + 2(\alpha+1)(\alpha+2) - 2(\alpha^2+3\alpha+4)$$

und basierend darauf, beweise, dass

$$5\mathfrak{o}_K = \mathfrak{p}\mathfrak{q}.$$

3.3 Bruchideale

Definition 3.3.1. Ein *Bruchideal* von $\mathfrak{o}_K$ ist eine nichtleere Teilmenge $\varnothing \neq I \subseteq K$, so dass für alle $x, y \in I$, $r \in \mathfrak{o}_K$:

1. $x + y \in I$;
2. $rx \in I$;
3. es eine natürliche Zahl $n \geq 1$ gibt, für den gilt

$$nI \subseteq \mathfrak{o}_K.$$

Wir benutzen die Notation $\mathcal{I}_K(\mathfrak{o}_K)$, oder einfach $\mathcal{I}_K$, für die Bruchideale von $\mathfrak{o}_K$.

Bemerkung 3.3.2. Man bemerke, dass wir *nicht* verlangen, dass ein Bruchideal multiplikativ abgeschlossen ist.

Direkt von der Definition folgen folgende Lemmas:

Lemma 3.3.3. *Sei $I \subseteq K$ ein Bruchideal von $\mathfrak{o}_K$, so dass $I \subseteq \mathfrak{o}_K$. Dann ist I ein Ideal.*

Lemma 3.3.4. *Sein I_α Bruchideale. Dann ist*

$$\bigcap_\alpha I_\alpha$$

ein Bruchideal.

Beweis. Dies ist einfach. Als Beispiel, bei Eigenschaft 3., wissen wir, dass für jeden I_α, es ein n_α gibt, mit $n_\alpha I_\alpha \subseteq \mathfrak{o}_K$. Man nehme irgend einen dieser $N \coloneqq n_\alpha$. Da der Schnitt eine Teilmenge von jedem I_α ist, gilt $N \cap_\alpha I_\alpha \subseteq NI_\alpha = n_\alpha I_\alpha \subseteq \mathfrak{o}_K$. □

Bemerkung 3.3.5. Achtung, wir können *nicht* schlussfolgern, dass wir von einem Bruchideal erzeugt mit einer beliebigen Menge $A \subseteq K$ sprechen können, da für K selber kein Bruchideal ist. (Dies kann man schon bei $K = \mathbb{Q}$ merken: Es gibt kein $n \in \mathbb{Z}$, mit $n\mathbb{Q} \subseteq \mathbb{Z}$). Es folgt, dass die Menge aller Bruchideale, welches eine Teilmenge $A \subseteq K$ enthält leer sein kann. Als solches kann man nicht einfach alle Bruchideale schneiden, welches A enthalten.

Wenn jedoch $A \subseteq I$ eine Teilmenge eines Bruchideals ist, dann kann man von (A), dem Bruchideal erzeugt mit A sprechen.

Lemma 3.3.6. *Die Bruchideale formen einen kommutativen Monoid unter der Verknüpfung*

$$\times : \mathcal{I}_K \times \mathcal{I}_K \to \mathcal{I}_K, \quad (I, J) \mapsto (ab \mid a \in I, b \in J),$$

wobei $(ab \mid a \in I, b \in J) = \{a_1 b_1 + \cdots + a_n b_n \mid a_i \in I,\ b_j \in J,\ n \in \mathbb{N}\}$ das Bruchideal erzeugt mit der Menge aller Produkte ist.

Beweis. Da $\{ab \mid a \in I, b \in J\} \subseteq I$ (natürlich liegt es auch in J), kann man ein Bruchideal mit dieser Menge erzeugen. Zuerst argumentieren wir, dass $(ab \mid a \in I, b \in J) = \{a_1 b_1 + \cdots + a_n b_n \mid a_i \in I,\ b_j \in J,\ n \in \mathbb{N}\}$. Da die rechte Seite in die linke liegt, muss man hier eigentlich nur beweisen, dass die rechte Seite ein Bruchideal ist. Die ersten zwei Eigenschaften sind klar. Bei dritten nehme man $n_I \times n_J$, wobei n_I (bzw. n_J) eine natürliche Zahl ist, welches die Eigenschaft der Definition erfüllt. Es gilt $n_I n_J (a_1 b_1 + \cdots + a_n b_n) = n_I a_1 n_J b_1 + \cdots + n_I a_n n_J b_n$, was nun von der Annahme ganzalgebraisch ist, da $n_I a_i$ und $n_J b_i$ ganzalgebraisch sind.

Das die Verknüpfung nun einen kommutativen Monoid formt (mit (1) als Einheit) wird genau wie bei normalen Idealen überprüft. □

Wir werden die Notation $\mathcal{I}^*$ (bzw. $\mathcal{I}_K^*$) für die Menge aller Ideale (bzw. Bruchideale) von $\mathfrak{o}_K$ außer (0) benutzen.

Lemma 3.3.7. *1. Die Menge $\mathcal{I}^*$ ist ein Monoid (unter dem Produkt);*

2. Die Menge $\mathcal{I}_K^*$ ist ein Monoid (unter dem Produkt).

Beweis. Aufgabe 63. □

Lemma 3.3.8. *Jedes Ideal $I \subseteq \mathfrak{o}_K$ ist auch ein Bruchideal in natürlicher weise. Das Produkt von Idealen geht dabei zum Produkt von Bruchidealen. Anders ausgedrückt: Die Einbettung $\mathfrak{o}_K \subseteq K$ induziert ein injektives Monoidhomomorphismus*

$$\Phi : \mathcal{I} \to \mathcal{I}_K.$$

Beweis. Aufgabe. □

Lemma 3.3.9. *Sei I ein Ideal von $\mathfrak{o}_K$. Dann definiert*

$$I^{-1} := \{x \in K \mid xI \subseteq \mathfrak{o}_K\}$$

ein Bruchideal.

Beweis. Aufgabe. □

Natürlich soll es das *Inverse* zu I sein. Wir müssen aber etwas arbeiten, um dies zu beweisen (und Sinn zu geben).

Lemma 3.3.10. *Sein $I, J \subseteq \mathfrak{o}_K$ Ideale.*

(i) Es gilt $J \subseteq I^{-1}J$.

(ii) Wir haben $(1)^{-1} = (1)$.

(iii) Aus $I \subseteq J$ folgt $J^{-1} \subseteq I^{-1}$.

(iv) Wir haben $\mathfrak{o}_K \subseteq I^{-1}$.

Beweis. (i) Bei Definition von I^{-1} gilt $1 \in I^{-1}$. Es folgt $J \ni x = 1 \cdot x \in I^{-1}J$.

(ii) Für jeden $x \in \mathfrak{o}_K$ ist $x(1) \subseteq \mathfrak{o}_K$, also $(1) \subseteq (1)^{-1}$. Auf der anderen Seite impliziert $x \in (1)^{-1}$, dass $x = x \cdot 1 \in \mathfrak{o}_K$, also $(1)^{-1} \subseteq (1)$.

(iii) & (iv) Diese folgen direkt von den Definition von I^{-1} und eines Ideals. □

Lemma 3.3.11. *Aus $I \subsetneq \mathfrak{o}_K$ folgt $\mathfrak{o}_K \subsetneq I^{-1}$.*

Beweis. Teile (ii) und (iii) von Lemma 3.3.10 kombinieren zu $I \subseteq \mathfrak{o}_K \Rightarrow \mathfrak{o}_K = \mathfrak{o}_K^{-1} \subseteq I^{-1}$. Es bleibt also zu beweisen, dass $I \neq \mathfrak{o}_K \Rightarrow \mathfrak{o}_K \neq I^{-1}$.

Jedes Ideal $I \neq (1)$ liegt in einem Maximalideal $I \subseteq \mathfrak{p} \subsetneq \mathfrak{o}_K$. Teile (ii) und (iii) von Lemma 3.3.10 besagen, dass $\mathfrak{o}_K \subseteq p^{-1} \subseteq I^{-1}$. Wenn wir also $\mathfrak{o}_k \neq \mathfrak{p}^{-1}$ beweisen, sind wir fertig. In anderen Worten, die Aussage lässt sich auf Maximalideale reduzieren.

Sei $a \in \mathfrak{p} \setminus \{0\}$ und sein $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ Maximalideale, so dass

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$$

gilt, mit r minimal. Wir können solche Maximalideale finden, laut Lemma 3.2.8. Daher gilt

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}.$$

Da ein Maximalideal auch prim ist (Korollar 1.1.50), impliziert Lemma 1.1.34, dass o. B. d. A,

$$\mathfrak{p}_1 \subseteq \mathfrak{p}.$$

Da $\mathfrak{p}_1$ jedoch maximal ist, muss

$$\mathfrak{p}_1 = p$$

gelten. Aufgrund der Minimalität von r muss auch

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq (a)$$

gelten. Daher gibt es ein

$$b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (a).$$

Für $r = 1$, also wenn $(a) = \mathfrak{p}$, nehme $b \in \mathfrak{o}_K \setminus (a)$. Wir behaupten, dass $\frac{b}{a} \in \mathfrak{p}^{-1} \setminus \mathfrak{o}_K$. Dies ist Wohldefiniert, da $a \neq 0$.

Um die Behauptung zu beweisen, bemerken wir zuerst, dass

$$\mathfrak{p}(b) \subseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a),$$

da $\mathfrak{p} = \mathfrak{p}_1$ und $(b) \subseteq \mathfrak{p}_2 \cdots \mathfrak{p}_r$. Im falle, wenn $(a) = \mathfrak{p}$ ist $\mathfrak{p}(b) \subseteq \mathfrak{p} = (a)$ bei Definition eines Primideals. Anders gesagt, für jeden $p \in \mathfrak{p}$ haben wir $pb = as, s \in \mathfrak{o}_K$. Es gilt

$$\frac{b}{a}\mathfrak{p} = \left\{ \frac{b}{a}p = \frac{as}{a} \in K \mid p \in \mathfrak{p} \right\} \subseteq \mathfrak{o}_K.$$

Wir schlussfolgern, dass

$$\frac{b}{a} \in \mathfrak{p}^{-1}.$$

Wenn $\frac{b}{a} \in \mathfrak{o}_K$, dann folgt aus der Definition eines Ideals, dass $b = \frac{b}{a}a \in (a)$ liegt, was aber unserer Annahme von b widerspricht. Dies schließt unseren Beweis ab. □

Lemma 3.3.12. *Sei $I \neq (0)$ ein Ideal von $\mathfrak{o}_K$. Ein Element $x \in K$ ist ganzalgebraisch (also $x \in \mathfrak{o}_K$), genau dann wenn $xI \subseteq I$.*

Beweis. Eine Seite is klar. Wenn $x \in \mathfrak{o}_K$, dann ist $xI = (x)I \subseteq I$. Für die andere Seite, erinnern wir uns an Korollar 2.4.7, laut welchem ein Ideal

$$I \subseteq \mathfrak{o}_K$$

eine endlich erzeugte freie (Abelsche) Gruppe ist. Daher,

$$I = \langle b_1, \ldots, b_n \rangle_{\mathbb{Z}}.$$

Da $xI \subseteq I$, können wir jedes Element von xI als eine Linearkombination der b_i's darstellen. Also

$$xb_i = \sum_j a_{i,j} b_j, \quad a_{i,j} \in \mathbb{Z}.$$

Sei A die Matrix $(a_{i,j})$. Wir haben

$$(A - x\mathsf{Id}_n) \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

wobei Id_n die Einheitsmatrix der Dimension $n \times n$ ist. Daher ist x ein Eigenwert von A. Da $b_i \in I \subseteq \mathfrak{o}_K$, $a_{i,j} \in \mathbb{Z} \subseteq \mathfrak{o}_K$ und ein Eigenwert dessen algebraische/polynomiale Kombination ist, ist $x \in \mathfrak{o}_K$. □

Korollar 3.3.13. *Sei $I \subseteq \mathfrak{o}_K$ ein Ideal und $J \subseteq K$ ein Bruchideal. Aus $I = JI$ folgt $J \subseteq \mathfrak{o}_K$.*

Beweis. Sei $J = (a_1, a_2, \ldots,)$ und $J' = (a_2, \ldots)$. Daher, $J = (a, J')$. Da, bei Definition, $JI = (xy \mid x \in (a_1) \text{ oder } x \in J,\ y \in I)$, folgt $a_1 I = (a_1)I \subseteq IJ$. $IJ = I$ impliziert spezifisch, dass $IJ \subseteq I$, was uns nun $a_1 I \subseteq I$ gibt. Lemma 3.3.12 besagt nun, dass $a_1 \in \mathfrak{o}_K$. Da aber a_1 ein beliebiges Element von J ist, gilt $J \subseteq \mathfrak{o}_K$. □

Lemma 3.3.14. *Sei $\mathfrak{p}$ ein Maximalideal von $\mathfrak{o}_K$. Dann gilt $\mathfrak{p}^{-1}\mathfrak{p} = (1)$.*

Beweis. Bei Definition von $\mathfrak{p}^{-1}$ gilt $\mathfrak{p}^{-1}\mathfrak{p} \subseteq \mathfrak{o}_K$ und von Teil (i), Lemma 3.3.3 (für $I = J = \mathfrak{p}$) folgt

$$\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p} \subseteq \mathfrak{o}_K.$$

Da $\mathfrak{p}$ ein Maximalideal ist gilt, $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ oder $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}_K = (1)$. Im ersten Fall führt Korollar 3.3.13 für $I = \mathfrak{p}$, $J = \mathfrak{p}^{-1}$ zu $\mathfrak{p}^{-1} \subseteq \mathfrak{o}_K$, was durch Lemma 3.3.11 nun ein Widerspruch gibt. Also $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}_K = (1)$. □

Satz 3.3.15. *Sei $(0) \neq I \subsetneq \mathfrak{o}_K$ ein Ideal von $\mathfrak{o}_K$. Es gibt Maximalideal $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, so dass*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Diese Zerlegung ist eindeutig bis auf Ordnung.

Beweis.

Existenz : Wir werden es durch eine "umgedrehte Induktion" beweisen. Sprich, wir werden zeigen, dass wenn es für große gilt, es auch für alle kleineren Ideale gelten muss.

Sei $I \neq (0)$ ein Ideal, so dass für alle Ideale $I \subsetneq J \neq \mathfrak{o}_K$, es eine Zerlegung in Maximalidealen gibt. Wir wollen zeigen, dass es auch für I eine solche Zerlegung geben muss.

Wenn I selbst ein Maximalideal ist, ist es klar erfüllt. Wenn nicht, ist es in einem Maximalideal $\mathfrak{p}$ enthalten, mit $I \subsetneq \mathfrak{p}$.
Behauptung: Es gilt

$$I \subsetneq \mathfrak{p}^{-1}I \subsetneq \mathfrak{o}_K.$$

Daraus wird direkt folgen, dass $\mathfrak{p}^{-1}I$ als Produkt von Maximalidealen dargestellt werden kann.

Aus $I \subseteq \mathfrak{p}$ folgt direkt aus Definition des Produkts, dass $\mathfrak{p}^{-1}I \subseteq \mathfrak{p}^{-1}\mathfrak{p}$. (Das es $\mathfrak{p}^{-1}$ ist macht hier keinen Unterschied, dies wäre für jede Teilmenge der Fall). Bei Lemmas 3.3.10 (Teil (i)) und 3.3.14 haben wir also

$$I \subseteq \mathfrak{p}^{-1}I \subseteq \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}_K.$$

Es bleibt zu Zeigen, dass die Inklusionen strikt sind. Sei $I = \mathfrak{p}^{-1}I$. Aus Korollar 3.3.13 folgt $p^{-1} \subseteq \mathfrak{o}_K$, was nach Teil (v) von Lemma 3.3.10 zu $\mathfrak{p} = (1)$ führt. Widerspruch. Es gilt also $I \subsetneq \mathfrak{p}^{-1}I$.

Wenn $\mathfrak{p}^{-1}I = \mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{o}_K$, dann folgt aus Lemma 3.3.14, dass $I = (\mathfrak{p}\mathfrak{p}^{-1})I = \mathfrak{p}(\mathfrak{p}^{-1}I) = \mathfrak{p}\mathfrak{o}_K = \mathfrak{p}$, was unserer Annahme widerspricht. Dies Beweist unsere Behauptung.

Bei Lemma 3.3.3 ist $\mathfrak{p}^{-1}I$ ein Ideal und es erfüllt unsere Induktionsannahme, daher zerfällt es in Maximalideale

$$\mathfrak{p}^{-1}I = \mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Indem wir nun beide Seiten mit $\mathfrak{p}$ multiplizieren (und es $\mathfrak{p}_1$ nennen), erhalten wir nach Anwendung von Lemma 3.3.14

$$I = \mathfrak{p}\mathfrak{p}^{-1}I = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Eindeutigkeit : Sei

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

mit $\mathfrak{p}_i, \mathfrak{q}_j$'s Maximalideale. Wir haben direkt, dass

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{q}_1,$$

woraus Lemma 1.1.34 (nach Umordnung) $\mathfrak{p}_1 \subseteq \mathfrak{q}_1$ impliziert, da maximal immer prim ist. Da es aber insbesondere maximal ist, folgt, dass

$$\mathfrak{p}_1 = \mathfrak{q}_1.$$

Indem wir beide Seiten mit $\mathfrak{p}_1^{-1}$ multiplizieren und Lemma 3.3.14 anwenden erhalten wir

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

Es ist nun direkt ersichtlich, wie man diese Aussage durch Induktion beweisen kann.

□

Satz 3.3.16. *Die Menge $\mathcal{I}_K^*$ der Bruchideale von $\mathfrak{o}_K$ ungleich Null, ist eine Abelsche Gruppe unter der Multiplikation.*

Beweis. Von Lemma 3.3.7 ausgehend müssen wir nur noch zeigen, dass jedes $I \in \mathcal{I}_K^*$ einen Inversen hat. Bei Definition gibt es einen $n \in \mathbb{Z} \subseteq \mathfrak{o}_K$, so dass $nI \subseteq \mathfrak{o}_K$ ein Ideal ist. Satz 3.3.15 besagt nun, dass es $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ gibt mit

$$nI = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Setze

$$I^{-1} := n\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}.$$

Dann haben wir

$$\begin{aligned} II^{-1} &= In\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} \\ &= nI\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} \\ &= \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} \\ &= (1). \end{aligned}$$

□

Nun folgen all die natürlichen Eigenschaften die von sich nicht trivial offensichtlich sind, wie z. B. $I = J$ *genau dann wenn* $I^{-1} = J^{-1}$, etc.. Satz 3.3.15 kann hier auch interpretiert werden, als "Maximalideale sind Erzeuger des Monoids $\mathcal{I}^*$, bzw. der Gruppe $\mathcal{I}_K^*$". Wir werden einige davon in den kommenden Aussagen geben:

Korollar 3.3.17. *Das Monoid $\mathcal{I}^*$ und die Gruppe $\mathcal{I}_K^*$ sind kürzbar.*

Beweis. Gruppen und deren Untermonoide sind immer kürzbar. □

Definition 3.3.18. Sein I, J Ideale von $\mathfrak{o}_K$. Dann heißt I ein Faktor von J, wenn es ein Ideal I' gibt, so dass $II' = J$. Wir schreiben $I \mid J$.

Korollar 3.3.19. $I \mid J$ *genau dann wenn* $J \subseteq I$.

Beweis. Eine Seite ist klar: aus $J = II'$ folgt $J \subseteq I$. Sei nun $J \subseteq I$. Da $\mathcal{I}_K^*$ eine Gruppe ist, gibt es ein Bruchideal $I' = \frac{J}{I}$, so dass $I'I = J \subseteq \mathfrak{o}_K$. Daher impliziert Lemma 3.3.12, dass $I' \subseteq \mathfrak{o}_K$, daher ein Ideal sein muss, was unseren Korollar beweist. □

Für Bruchideale stimmt es natürlich nicht. Sei $\mathfrak{o}_K \subsetneq I$ ein Bruchideal, dass echt größer ist als $(1) = \mathfrak{o}_K$. Dann ist $(1)I = I \not\subseteq (1)$.

Proposition 3.3.20. *Die Konstruktion in Lemma 3.3.9 ist tatsächlich das Inverse eines Ideals.*

Beweis. Nur für diesen Beweis, bezeichnen wir $I^* := \{x \mid xI \subseteq \mathfrak{o}_K\}$. Wie gewohnt ist I^{-1} das Inverse von I, im Sinne der Gruppenstruktur, daher $II^{-1} = (1)$. Es gilt zu beweisen, dass $I^* = I^{-1}$. Laut Lemma 3.3.14 gilt dies für Maximalideale und da wir jedes Ideal als Produkt von Maximalidealen zerlegen können (Satz 3.3.15) muss man nur beweisen, dass die Konstruktion I^* mit dem Produkt verträglich ist: Wir machen den Fall $(\mathfrak{pq})^* = \mathfrak{p}^*\mathfrak{q}^*$. Der Unterschied im allgemein Fall ist hauptsächlich Notation.

Es ist direkt klar, dass $\mathfrak{p}^*\mathfrak{q}^* = \{x_1y_1 + \cdots + x_ny_n \mid x_i\mathfrak{p} \subseteq \mathfrak{o}_K,\ y_i\mathfrak{q} \subseteq \mathfrak{o}_K\} \subseteq (\mathfrak{pq})^* = \{z \mid z\mathfrak{pq} \subseteq \mathfrak{o}_K\}$. Auf der andern Seite haben wir $\mathfrak{p}^*\mathfrak{q}^* = \mathfrak{p}^{-1}\mathfrak{q}^{-1} = (\mathfrak{pq})^{-1}$, laut Lemma 3.3.14. Zusammengefasst

$$(\mathfrak{pq})^{-1} = \mathfrak{p}^*\mathfrak{q}^* \subseteq (\mathfrak{pq})^*.$$

Da aber für jedes Ideal I gilt $I^* \subseteq I^{-1}$, folgt

$$(\mathfrak{pq})^* \subseteq (\mathfrak{pq})^{-1} = \mathfrak{p}^*\mathfrak{q}^*,$$

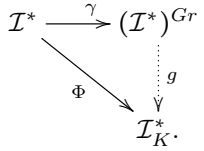
also Gleichhaut. □

Satz 3.3.21. *Die Gruppe $\mathcal{I}_K^*$ ist die Grothendieck Gruppe (Quotientengruppe) von $\mathcal{I}^*$.*

Beweis. In anderen Worten, wir wollen zeigen, dass

$$(\mathcal{I}^*)^{Gr} \simeq \mathcal{I}_K^*.$$

Wir erinnern uns an Korollar 1.2.8 was besagt, dass es ein eindeutiges Monoidhomomorphismus $g : (\mathcal{I}^*)^{Gr} \to \mathcal{I}_K^*$ gibt, so dass das folgende Diagramm kommutiert:



Es gilt zu beweisen, dass g eine Bijektion ist. Dafür werden wir folgende Behauptung benutzen: Behauptung: Für $0 \neq I$ Ideal gilt $g(\gamma(I)) = \frac{1}{\Phi(I)}$. Wir haben

$$1 = g(1) = g\left(\frac{I}{I}\right) = g\left(\frac{I}{1}\right) g\left(\frac{1}{I}\right) = g(\gamma(I)) g\left(\frac{1}{I}\right) = \Phi(I) g\left(\frac{1}{I}\right)$$

woraus

$$g\left(\frac{1}{I}\right) = \frac{1}{\Phi(I)}$$

folgt, da $\mathcal{I}_K^*$ eine Gruppe ist. (Mann kann nicht $\frac{\Phi(I)}{\Phi(J)} = \Phi\left(\frac{I}{J}\right)$ schreiben, da $\frac{I}{J}$ im allgemeinen nicht in $\mathcal{I}^*$ liegt.

Nun zum Beweis: Sein $I, J \in \mathcal{I}^*$ Ideale von $\mathfrak{o}_K$ ungleich Null.
Injektion: Sei $g\left(\frac{I}{J}\right) = 1$, also

$$1 = g\left(\frac{I}{1}\right) g\left(\frac{1}{J}\right) = g(\gamma(I)) \frac{1}{\Phi(J)} = \Phi(I) \frac{1}{\Phi(J)} = \frac{\Phi(I)}{\Phi(J)}.$$

Die impliziert sofort

$$\Phi(J) = \Phi(I)$$

was $J = I$ ergibt, da f injektiv ist. Daher ist $\frac{I}{J} = \frac{I}{I} = 1$ also ist auch g injektiv.
Surjektion: Sei $I \in \mathcal{I}_K^*$ ein Bruchideal. Wir wissen, dass es ein $n \in \mathbb{Z} \subseteq \mathfrak{o}_K$ gibt, so dass $nI \in \mathcal{I}^*$ ein Ideal ist. Daher haben wir

$$g\left(\frac{nI}{n}\right) = \frac{g(\gamma(nI))}{g(\gamma(n))} = \frac{\Phi(nI)}{\Phi(n)} = \frac{\Phi(n)\Phi(I)}{\Phi(n)} = \Phi(I) = I.$$

Mit $\gamma(n)$ meinen wir eigentlich $\gamma((n))$. Es folgt, dass $\frac{nI}{n} \in (\mathcal{I}^*)^{Gr}$ nach I abbildet, was Surjektivität beweist. □

Aufgaben

Aufgaben 11

Aufgabe 63 (1 Punkt). Zur Erinnerung, für einen Zahlenring $\mathfrak{o}_K$, bezeichnen wir mit $\mathcal{I}^*$ die Menge der Ideale von $\mathfrak{o}_K$ ungleich Null. Mit $\mathfrak{o}_K^*$ bezeichnen wir die Menge der Bruchideale ungleich Null. Beweise folgende Aussagen:

1. Die Menge $\mathcal{I}^*$ ist ein Monoid (unter dem Produkt);
2. Die Menge $\mathcal{I}_K^*$ ist ein Monoid (unter dem Produkt).

Aufgabe 64 (2 Punkte). Sei $\mathfrak{o}_K = \mathbb{Z}$. Entscheide, mit Begründung, welche dieser Mengen ein Bruchideal definiert:

i) $\frac{1}{2}\mathbb{Z} = \left\{\frac{n}{2}, n \in \mathbb{Z}\right\}$

ii) $\mathbb{Z}_2 = \left\{\frac{n}{2^m}, n, m \in \mathbb{Z}\right\}$

iii) $\mathbb{Z}_{\langle 2\rangle} = \left\{\frac{n}{2m}, n, m \in \mathbb{Z}\right\}$

iv) $\mathbb{Z}_{(2)} = \left\{\frac{n}{2m+1}, n, m \in \mathbb{Z}\right\}$

Aufgabe 65 (4 Punkte). Berechne die Inverse der folgenden Ideale:

i) (1 Teilpunkt) $\mathfrak{a} = (2) \subseteq \mathfrak{o}_{\mathbb{Q}}$,

ii) (1 Teilpunkt) $\mathfrak{b} = (2) \subseteq \mathfrak{o}_K$, mit $K = \mathbb{Q}(\sqrt{3})$,

iii) (1 Teilpunkt) $\mathfrak{c} = (\sqrt{3}) \subseteq \mathfrak{o}_K$, mit $K = \mathbb{Q}(\sqrt{3})$,

iv) (1 Teilpunkt) $\mathfrak{d} = (2, \sqrt{3}) \subseteq \mathfrak{o}_K$, mit $K = \mathbb{Q}(\sqrt{3})$.

Aufgabe 66 (3 Punkte). Sei $\mathfrak{o}_K = \mathbb{Z}[\sqrt{-6}]$ mit Ganzheitsbasis $\{1, \sqrt{-6}\}$. Betrachte die Ideale $\mathfrak{a} = (2, \sqrt{6})$ und $\mathfrak{b} = (3, \sqrt{-6})$).

i) (1 Teilpunkt) Sind $\mathfrak{a}, \mathfrak{b}$ Maximalideale?

ii) (2 Teilpunkte) Berechne das Bruchideal $\mathfrak{a}^{-1}\mathfrak{b}$.

Die folgende Aufgabe ist recht schwer und das Stoff ist außerhalb der Grenzen/Interesse des Kurses! Es sollte wie eine "Sonderaufgabe" behandelt werden.

Ein Noetherscher Ring R heißt *Dedekindring*, wenn es ein Integritätsbereich ist und jedes Ideal eine Zerlegung in Primideale hat. Das heißt, wenn für jeden $\mathfrak{a} \subseteq R$, es Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, so dass

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n.$$

Diese Zerlegung wird dann eindeutig sein (dies kann Bewiesen werden). Für Dedekindringe kann man Bruchideale genau so wie für Zahlenringe einführen und die Bruchideale eines Dedekindringes bilden eine Gruppe unter der Multiplikation, mit $R = (1)$ als die Einheit.

Aufgabe 67 (5 Punkte). Sei R ein Dedekindring und $S \subseteq R$ ein Untermonoid.

i) (2 Teilpunkte) Beweise, dass die Lokalisation $S^{-1}R$ ein Dedekindring ist.

ii) (3 Teilpunkte) Sei $\mathfrak{a} \subseteq R$ ein Bruchideal von R.

ii a) Zeige, dass $S^{-1}\mathfrak{a}$ ein Bruchideal von $S^{-1}R$ ist.

ii) b) Zeige, dass die Abbildung $\mathfrak{a} \mapsto S^{-1}\mathfrak{a}$ einen Gruppenhomomorphismus zwischen den Bruchidealen von R und den Bruchidealen von $S^{-1}R$ definiert.

3.4 Norm von Idealen

Zu Erinnerung, wir definierten die Norm eines Ideals als

$$\mathsf{N}(I) = |\mathfrak{o}_K/I|,$$

die Anzahl der Elemente des Quotientenringes.

Satz 3.4.1. *Sein $I, J \subseteq \mathfrak{o}_K$ Ideale. Dann gilt*

$$\mathsf{N}(IJ) = \mathsf{N}(I)\mathsf{N}(J).$$

Beweis. Da wir J als Produkt von Maximalidealen zerlegen können (Satz 3.3.15), dürfen wir Annehmen, dass $J = \mathfrak{p}$ selber ein Maximalideal ist. (Der Rest ist dann Induktion indem wir I mit $I \cdot \mathfrak{p}_i$ ersetzen). Der zweite Isomorphiesatz 1.1.47 besagt

$$\mathfrak{o}_K/I \simeq (\mathfrak{o}_k/I\mathfrak{p}) \,/\, (I/I\mathfrak{p}) \,.$$

Als solches gilt laut Lagrange

$$\mathsf{N}\,(I) = N\,(I\mathfrak{p})\,/|I/I\mathfrak{p}|,$$

wobei $|\cdot|$ die Anzahl der Elemente bezeichnet. Daher verbleibt es zu zeigen, dass

$$\mathsf{N}\,(\mathfrak{p}) = |I/I\mathfrak{p}|.$$

Hierzu nehmen wir ein Element $a \in I \setminus I\mathfrak{p}$. So ein Element gibt es, da sonst $I = I\mathfrak{p} \Rightarrow (1) = \mathfrak{p}$ folgen würde (Korollar 3.3.17). Definiere die Abbildung

$$\Phi_a : \mathfrak{o}_K \to I/I\mathfrak{p} \quad \text{gegeben durch} \quad \Phi_a(x) = ax + I\mathfrak{p}.$$

Wir behaupten das diese Abbildung surjektiv ist. Um dies zu sehen, bemerken wir zuerst, dass es keinen Ideal zwischen $I\mathfrak{p}$ und I gibt, da $\mathfrak{p}$ Maximal ist. Denn wenn $I\mathfrak{p} \subsetneq A \subsetneq I$ gilt, dann folgt von Satz 3.3.16 und Korollar 3.3.17, dass

$$\mathfrak{p} = I^{-1}I\mathfrak{p} \subsetneq I^{-1}A \subsetneq I^{-1}I = \mathfrak{o}_K,$$

was der Maximalität von $\mathfrak{p}$ widerspricht. Daher ist $I = (a, I\mathfrak{p})$, also als Ideal durch a und $I\mathfrak{p}$ erzeugt. Dies impliziert nun Surjektivität, da also jedes Element von der Form $ax + b, b \in I\mathfrak{p}$ ist.

Nun wollen wir den Kern bestimmen. Sei $x \in \mathfrak{p} \subseteq \mathfrak{o}_K$. Dann ist $ax \in I\mathfrak{p}$, was uns $\Phi_a(x) = 0 + I\mathfrak{p}$ gibt. Also bildet ganz $\mathfrak{p}$ auf die Null ab. Daher $\mathfrak{p} \subseteq \mathsf{Ker}(\Phi_a) \subseteq \mathfrak{o}_K$. Da $\mathsf{Ker}(\Phi_a)$ ein Ideal von $\mathfrak{o}_K$ ist (Proposition 1.1.45) und $\mathfrak{p}$ maximal ist, muss $\mathsf{Ker}(\Phi_a) = \mathfrak{p}$ oder $\mathsf{Ker}(\Phi_a) = \mathfrak{o}_K$ gelten. Da aber

$$\Phi_a(1) = a + I\mathfrak{p} \neq 0 + I\mathfrak{p} \quad \text{da} \quad a \notin I\mathfrak{p},$$

muss $\mathsf{Ker}(\Phi_a) = \mathfrak{p}$ sein.

Der Hauptisomorphiesatz 1.1.46 sagt nun, dass

$$\mathfrak{o}_K/\mathfrak{p} \simeq \mathsf{Bild}(\Phi_a) = I/I\mathfrak{p},$$

was

$$\mathsf{N}(\mathfrak{p}) = |I/I\mathfrak{p}|,$$

und damit unseren Satz, impliziert. □

Lemma 3.4.2. *Sei $\varphi : K \to L$ ein Ringhomomorphismus zwischen algebraischen Zahlenkörpern. Dann ist $\varphi(\mathfrak{o}_K) \subseteq \mathfrak{o}_L$. Anders ausgedrückt, die Einschränkung*

$$\varphi|_{\mathfrak{o}_K} : \mathfrak{o}_K \to \mathfrak{o}_L$$

definiert einen Ringhomomorphismus.

Beweis. Sei $\alpha \in \mathfrak{o}_K$. Daher, es gibt ein normiertes Polynom $f(x) \in \mathbb{Z}[X]$, so dass $f(\alpha) = 0$. Da

$$f(\varphi(x)) = \varphi(f(x)) = \varphi(0) = 0$$

folgt unsere Aussage. (Anders ausgedrückt, jede polynomiale Gleichung die von α erfüllt wird, muss auch von $\sigma(\alpha)$ erfüllt werden. □

Lemma 3.4.3. *Sei $\sigma : K \to K$ ein Endomorphismus. Dann sind σ und $\sigma|_{\mathfrak{o}_K}$ Automorphismen. Spezifisch, gibt es eine Gleichheit (nicht nur Isomorphie) von Teilmengen von K*

$$\mathfrak{o}_K = \sigma(\mathfrak{o}_K).$$

Beweis. Man kann dies Mithilfe des ersten Isomorphiesatzes schlussfolgern, mit Dimensionsargumenten. Alternativ kann man es auch mit lineare Algebra machen (die Grundideen sind die selben):

Nach vergessen der Ringstruktur ist K ein endliches $\mathbb{Q}$-Vektorraum und σ ein Vektorraumhomomorphismus. Proposition 1.1.52 besagt, dass dies ein Injektiver Vektorraumhomomorphismus ist. Daher ist es eine Isomorphie als $\mathbb{Q}$-Vektorräume, daher auch als Körper. (Das Argument ist die selbe, wie bei endlichen Mengen).

Da es eine Isomorphie ist, wird alles "algebraische" respektiert werden, daher auch die Einschränkung. (Wenn es nicht klar ist, sollte man sich per Hand davon überzeugen).

Der letzte Teil dieser Aussage folgt von unserem Argument in Lemma 3.4.2. □

Bemerkung 3.4.4. Achtung, die Gleichheit $\mathfrak{o}_K = \sigma(\mathfrak{o}_K)$ in Lemma 3.4.3 heißt nicht, dass $\sigma|_{\mathfrak{o}_K}$ die Identität ist. Nur, dass es die selben Teilmengen von K sind.

Proposition 3.4.5. *Sei $\sigma : K \to K$ ein Endomorphismus.*

i) Sei $I \in \mathcal{I}_K$ ein Bruchideal von $\mathfrak{o}_K$. Das Bild $\sigma(I) \in \mathcal{I}_K$ ist ein Bruchideal von $\mathfrak{o}_K$.

ii) Sei $J \in \mathcal{I}_K$ ein Bruchideal von $\mathfrak{o}_K$. Das Uhrbild $\sigma^{-1}(J) \in \mathcal{I}_K$ ist ein Bruchideal von $\mathfrak{o}_K$.

Beweis. Aufgabe/Korollar von Lemma 3.4.3. □

Bemerkung 3.4.6. Wenn I bzw., J ein Ideal ist, so ist dessen Bild bzw. Uhrbild auch ein Ideal. Dies folgt von Teil i) dieser Proposition und Lemma 3.3.3.

Korollar 3.4.7. *Sei $\sigma : K \to K$ ein Endomorphismus und $I \subseteq \mathfrak{o}_K$ ein Ideal. Dann gilt*

$$\mathsf{N}(I) = \mathsf{N}(\sigma(I)) = \mathsf{N}(\sigma^{-1}(I)).$$

Beweis. Folgt von der Tatsache, dass σ eine Isomorphie ist, Lemma 3.4.3. Genauer

$$\mathsf{N}(I) = |\mathfrak{o}_K/I| = |\mathfrak{o}_K/I| = |\sigma(\mathfrak{o}_K)/\sigma(I)| = |\mathfrak{o}_K/\sigma(I)| = \mathsf{N}(\sigma(I)|,$$

wobei die vierte Gleichung gilt, da $\sigma(\mathfrak{o}_K) = \mathfrak{o}_K$, laut Lemma 3.4.2. Das gleiche gilt auch für σ^{-1}, da es eine Isomorphie ist. □

Bemerkung 3.4.8. Wir bemerken, dass $\mathfrak{o}_K = \sigma(\mathfrak{o}_K)$, aber $I \simeq \sigma(I)$ nur eine Isomorphie ist. Z. B., sie $\sigma : \mathbb{Q}(i) \to \mathbb{Q}(i)$ gegeben durch $a + bi \mapsto a - bi$. Dann sind $(1 + 2i)$ und $(1 - 2i)$ "sehr ähnlich", sie haben keinerlei "strukturelle Unterschiede" (es gibt keine Eigenschaft die man für allgemeine Ringe sagen kann, dass das eine hat, das andere jedoch nicht). Diese sind aber nicht *gleich* als Mengen, denn $1 + 2i \notin (1 - 2i)$.

Wir können Korollar 3.4.7 öfters benutzen, um Normen von Idealen einfach auszurechnen:

Beispiel 3.4.9. Wir wollen die Norm von $(2, 1+\sqrt{3})$ berechnen. Es gilt

$$\begin{aligned}
\mathsf{N}(2,1+\sqrt{3})^2 &= \mathsf{N}(2,1+\sqrt{3})\mathsf{N}(2,1+\sqrt{3}) \\
&= \mathsf{N}(2,1+\sqrt{3})\mathsf{N}(2,1-\sqrt{3}) \\
&= \mathsf{N}(4,2-2\sqrt{3},2+2\sqrt{3},-2) \\
&= \mathsf{N}((2)) \\
&= 4
\end{aligned}$$

Die letzte Gleichung kommt von Korollar 3.4.17. Wir haben $\mathsf{N}((2))$ geschrieben, um es von der Norm des Elements 2 zu Unterscheiden. Korollar 3.4.17 wird uns bald ermöglichen, die Klammer wegzulassen.

Da $\mathsf{N}(2,1+\sqrt{3})^2 = 4$ und die Norm eines Ideals positiv ist, muss $\mathsf{N}(2,1+\sqrt{3}) = 2$ gelten.

Wir werden den folgen Satz nicht beweisen, da es von der linearen Algebra bekannt sein sollte. Der Beweis wird als solches auch nicht abgeprüft.

Satz 3.4.10. *Sei G eine freie Abelsche Gruppe mit Basis $\mathcal{B} = \{b_1, \dots, b_d\}$ und H eine Untergruppe, so dass $|G/H| < \infty$ endlich ist. Es gibt linear unabhängige Elemente $\mathcal{C} = \{c_1, \dots, c_d\} \subseteq G$, so dass*

$$H = \langle c_1, \dots, c_d \rangle_{\mathbb{Z}}$$

und

$$|G/H| = |\det(M_{\mathcal{C}}^{\mathcal{B}})|,$$

wobei $M_{\mathcal{C}}^{\mathcal{B}}$ die Basiswechselmatrix von $\mathcal{B}$ nach $\mathcal{C}$ ist.

Bemerkung 3.4.11. Zur Erinnerung, mit $\langle c_1, \dots, c_d \rangle_{\mathbb{Z}}$ meinen wir die abelsche Gruppe erzeugt mit den Elementen $c_1, \dots, c_d$. Anders gesagt

$$\langle c_1, \dots, c_d \rangle_{\mathbb{Z}} = \sum_{i=1}^{d} n_i c_i \quad n_i \in \mathbb{Z}.$$

Definition 3.4.12. Sei $I \subseteq \mathfrak{o}_K$ ein Ideal. Wir sagen, dass $\{c_1, \dots, c_d\}$ eine *Ganzheitsbasis* von I ist, wenn die c_i's linear Unabhängig über $\mathbb{Q}$ sind und

$$I = \langle c_1, \dots, c_d \rangle_{\mathbb{Z}} = \sum_{i=1}^{d} n_i c_i \quad n_i \in \mathbb{Z}$$

gilt.

Bemerkung 3.4.13. Wenn $\{c_1, \dots, c_d\}$ eine Ganzheitsbasis von I ist, dann gilt $I = (c_1, \dots, c_d)$. Aber, wenn $I = (a_1, \cdots, a_n)$ das Ideal erzeugen, muss $\{a_1, \cdots, a_n\}$ keine Ganzheitsbasis von I sein, auch wenn die a_i's linear unabhängig sind. Sei z. B., $K = \mathbb{Q}(\sqrt{2})$, mit $\mathfrak{o}_K = \mathbb{Z}[\sqrt{2}]$. Man betrachte die Ideale $I = (1)$ und $J = (\sqrt{2})$. Weder $\mathcal{B} = \{1\}$, noch $\mathcal{C} = \{\sqrt{2}\}$ sind Ganzheitsbasen, denn $\sqrt{2} \in I$, aber $\sqrt{2} \neq n \cdot 1$, mit $n \in \mathbb{Z}$ und $2 \in J$, aber $2 \neq n\sqrt{2}$, mit $n \in \mathbb{Z}$.

Bemerkung 3.4.14. Wir hatten diese Definition schon im Arbeitsblatt. Da diese das Ideal I als Abelsche Gruppe erzeugen, werden diese auch eine $\mathbb{Q}$-Basis von K bilden. Die Diskriminante ist genau die selbe, wie in Definition 2.2.11 gegeben.

Wir benutzen Satz 3.4.10 um folgende Proposition zu beweisen:

Proposition 3.4.15. *Sei $\mathfrak{o}_K$ ein Zahlenring, $\mathcal{B} = \{b_1, \dots, d_d\}$ eine Ganzheitsbasis von $\mathfrak{o}_K$ und $(0) \neq I \subseteq \mathfrak{o}_K$ ein Ideal. Es gibt eine Ganzheitsbasis $\mathcal{C} = \{c_1 \dots, c_d\}$ von I und es gilt*

$$\mathsf{N}(I) = \sqrt{\frac{\Delta(\mathcal{C})}{\Delta(\mathcal{B})}}.$$

Beweis. Bei Definition ist $\mathsf{N}(I) = |\mathfrak{o}_K/I|$. Laut Korollar 2.4.5 ist $\mathfrak{o}_K$ eine freie Abelsche Gruppe vom Rang d. Wir wissen, dass dieser Quotient immer endlich ist (Proposition 3.2.2). Daher gibt es laut Satz 3.4.10 eine Ganzheitsbasis $\mathcal{C} = \{c_i\}_{i=1}^d \subseteq I \subseteq \mathfrak{o}_K$'s, so dass

$$I = \langle c_1, \dots, c_d \rangle_{\mathbb{Z}}$$

und

$$\mathsf{N}(I) = |\mathfrak{o}_K/I| = |\det(M_{\mathcal{C}}^{\mathcal{B}})|,$$

wobei $M_{\mathcal{C}}^{\mathcal{B}}$ die Basiswechselmatrix von $\mathcal{B}$ nach $\mathcal{C}$ ist. Korollar 2.2.18 sagt aus, dass

$$\det(M_{\mathcal{C}}^{\mathcal{B}}) = \sqrt{\frac{\Delta(\mathcal{C})}{\Delta(\mathcal{B})}}$$

was nun zu

$$\mathsf{N}(I) = |\mathfrak{o}_K/I| = |\det(M_{\mathcal{C}}^{\mathcal{B}})| = \sqrt{\frac{\Delta(\mathcal{C})}{\Delta(\mathcal{B})}}$$

zusammenfügt. □

Ganzheitsbasen von Hauptidealen sind sehr einfach zu finden, wenn man schon eine Ganzheitsbasis von $\mathfrak{o}_K$ kennt.

Lemma 3.4.16. *Sei $\mathcal{B} = \{b_1, \dots, b_d\}$ eine Ganzheitsbasis von $\mathfrak{o}_K$, $a \in \mathfrak{o}_K$ und (a) das Hauptideal dazu. Dann ist $a\mathcal{B} = \{ab_1, \dots, ab_d\}$ eine Ganzheitsbasis von (a).*

Beweis. Aufgabe. □

Wir haben nun zwei Normen kennen gelernt, von Idealen und von Elementen. Diese sind wie folgt miteinander verbunden:

Korollar 3.4.17. *Sei $a \in \mathfrak{o}_K$ ein Element und (a) das Hauptideal dazu. Es gilt*

$$\mathsf{N}((a)) = |\mathsf{N}(a)|.$$

Beweis. Sei $\mathcal{B}$ eine Ganzheitsbasis von $\mathfrak{o}_K$. Laut Lemma 3.4.16 ist $a\mathcal{B}$ eine Ganzheitsbasis von (a) und wir haben

$$\Delta(a\mathcal{B}) = \det(\sigma_i(ab_j))^2 = \mathsf{N}(a)^2 \det(\sigma_i(b_j))^2 = \mathsf{N}(a)^2 \Delta(\mathcal{B}).$$

Proposition 3.4.15 für $\mathcal{C} = a\mathcal{B}$ impliziert nun, dass

$$\mathsf{N}((a)) = \sqrt{\frac{\Delta(a\mathcal{B})}{\Delta(\mathcal{B})}} = \sqrt{\frac{\mathsf{N}(a)^2\Delta(\mathcal{B})}{\Delta(\mathcal{B})}} = |\mathsf{N}(a)|.$$

□

Bemerkung 3.4.18. Um die zweite Gleichung $\det(\sigma_i(ab_j))^2 = \mathsf{N}(a)^2 \det(\sigma_i(b_j))^2$ etwas klarer zu machen, sei $\mathcal{B} = \{u, v, w\}$. Dann gilt

$$\begin{aligned}
\det\begin{pmatrix} \sigma_1(au) & \sigma_2(au) & \sigma_3(au) \\ \sigma_1(av) & \sigma_2(av) & \sigma_3(av) \\ \sigma_1(aw) & \sigma_2(aw) & \sigma_3(aw) \end{pmatrix} &= \det\left(\begin{pmatrix} \sigma_1(u) & \sigma_2(u) & \sigma_3(u) \\ \sigma_1(v) & \sigma_2(v) & \sigma_3(v) \\ \sigma_1(w) & \sigma_2(w) & \sigma_3(w) \end{pmatrix}\begin{pmatrix} \sigma_1(a) & 0 & 0 \\ 0 & \sigma_2(a) & 0 \\ 0 & 0 & \sigma_3(a) \end{pmatrix}\right) \\
&= \det\begin{pmatrix} \sigma_1(u) & \sigma_2(u) & \sigma_3(u) \\ \sigma_1(v) & \sigma_2(v) & \sigma_3(v) \\ \sigma_1(w) & \sigma_2(w) & \sigma_3(w) \end{pmatrix}\det\begin{pmatrix} \sigma_1(a) & 0 & 0 \\ 0 & \sigma_2(a) & 0 \\ 0 & 0 & \sigma_3(a) \end{pmatrix} \\
&= \det\begin{pmatrix} \sigma_1(u) & \sigma_2(u) & \sigma_3(u) \\ \sigma_1(v) & \sigma_2(v) & \sigma_3(v) \\ \sigma_1(w) & \sigma_2(w) & \sigma_3(w) \end{pmatrix} \cdot \mathsf{N}(a)
\end{aligned}$$

Das gilt natürlich für beliebig viele Basiselemente.

Man vergleiche das folgende Resultat zu Korollar 3.0.3:

Lemma 3.4.19. *Sei $I \subseteq \mathfrak{o}_k$ ein Ideal. Dann gilt*

$$\mathsf{N}(I) \in I.$$

Beweis. Sei $\mathsf{N}(I) = |\mathfrak{o}_K/I| = n$. Laut dem Satz von Lagrange (dem kleinen Satz von Fermat) gilt $n\overline{x} = 0$ für jeden $\overline{x} \in \mathfrak{o}_K/I$. Daher, $n\overline{1} = \overline{n} = 0$. Dies jedoch ist äquivalent zu sagen, dass $n \in I$, was wir beweisen wollten. □

Korollar 3.4.20. *Sei $I \subseteq \mathfrak{o}_K$. Dann ist $\mathsf{N}(I) = 1$ genau dann, wenn $I = (1) = \mathfrak{o}_K$.*

Beweis. Direktes Korollar von Lemma 3.4.19 und Korollar 1.1.13. □

Korollar 3.4.21. *Sei $I \subseteq J$ mit $\mathsf{N}(I) = \mathsf{N}(J)$. Dann gilt $I = J$.*

Beweis. Beweis ist eine Zusammenführung unserer vorigen Resultate: Aus Korollar 3.3.19 folgt, dass es ein I' gibt mit $II' = J$. Satz 3.4.1 besagt, dass $\mathsf{N}(J) = \mathsf{N}(II') = \mathsf{N}(I)\mathsf{N}(I') = \mathsf{N}(I)$. Daher gilt $\mathsf{N}(I') = 1$, woraus Korollar 3.4.20 impliziert, dass $I' = (1)$, also $J = II' = I(1) = I$. □

Korollar 3.4.22. *Für jeden $n \in \mathbb{Z}$ gibt es nur endlich viele Ideale $I \subseteq \mathfrak{o}_K$ mit $\mathsf{N}(I) = n$.*

Beweis. Da $\mathsf{N}(I) \in I$ (Lemma 3.4.19) folgt, dass $(n) \subseteq I$. Daher $I \mid (n)$ (Korollar 3.3.19). Da es aber eine eindeutige Zerlegung von Idealen gibt (Satz 3.3.15), hat jedes Ideal (einschließlich (n)) nur endlich viele Teiler. (Der Grund dafür ist, dass die Norm multiplikativ ist und sich also mit jedem Teiler verkleinert). □

3.4.1 Norm von Primidealen

Man erinnere sich, dass das Uhrbild eines Primideals wieder ein Primideal ist, Proposition 1.1.38. Für jeden algebraischen Zahlenring $\mathfrak{o}_K$ haben wir $\mathbb{Z} \subseteq \mathfrak{o}_K$. Eine Einbettung kann man natürlich auch als einen injektiven Ringhomomorphismus ι auffassen. Proposition 1.1.38 besagt, dass $\iota^{-1}(\mathfrak{p}) = \mathbb{Z} \cap \mathfrak{p}$ ein Primideal von $\mathbb{Z}$ ist, für jeden Primideal $\mathfrak{p} \in \mathfrak{o}_K$. In anderen Worten, $\mathbb{Z} \cap \mathfrak{p} = (p)$ oder $\mathbb{Z} \cap \mathfrak{p} = (0)$.

Lemma 3.4.23. *Genau dann ist $\mathbb{Z} \cap \mathfrak{p} = (0)$, wenn $\mathfrak{p} = (0)$.*

Beweis. Dass $\mathfrak{p} = (0) \Rightarrow \mathbb{Z} \cap \mathfrak{p} = (0)$ ist klar. Sei $\mathfrak{p} \neq (0)$. Daher, es gibt ein $0 \neq \alpha \in \mathfrak{p}$. Da $\mathfrak{m}_\alpha = a_0 + a_1 x + \cdots + x^n$ irreduzibel ist, muss $a_0 \neq 0$ sein (sonst könnten wir es durch x teilen). Als solches ist $0 \neq a_0 = -\alpha\left(a_1 + \cdots + a_n\alpha^{n-1}\right) \in \mathfrak{p}$ und wir sind fertig. □

Definition 3.4.24. Sei $\mathfrak{p} \subseteq \mathfrak{o}_K$ ein Primideal und lass $(p) = \mathbb{Z} \cap \mathfrak{p}$. Wir sagen, dass $\mathfrak{p}$ *über p liegt* und schreiben $\mathfrak{p} \mid p$.

Bemerkung 3.4.25. Um die Notation $\mathfrak{p} \mid p$ zu erklären, liege $\mathfrak{p}$ über p. Da $\mathbb{Z}$ in kanonischer Art ein Unterring von jedem $\mathfrak{o}_K$ ist, können wir $p \in \mathbb{Z}$ auch als ein Element $p \in \mathfrak{o}_K$ auffassen. Daher, können wir auch das Hauptideal $(p)_{\mathfrak{o}_K} \subseteq \mathfrak{o}_K$ erzeugt von p, aber in $\mathfrak{o}_K$ betrachten. (Wir schreiben hier $(p)_{\mathfrak{o}_K}$ um es von $(p) \subseteq \mathbb{Z}$ zu unterscheiden). Da $p \in (p) = \mathbb{Z} \cap \mathfrak{p}$, ist $p \in \mathfrak{p}$ und daher $(p)_{\mathfrak{o}_K} \subseteq \mathfrak{p}$. Laut Korollar 3.3.19 haben wir also, dass $\mathfrak{p} \mid (p)_{\mathfrak{o}_K}$.

Proposition 3.4.26. *Sei $(0) \neq \mathfrak{p} \subseteq \mathfrak{o}_K$ ein Ideal.*

$$\mathsf{N}(\mathfrak{p}) = p \text{ Primzahl } \Rightarrow \mathfrak{p} \text{ Primideal}.$$

Beweis. Sei $\mathfrak{p}$ ein Ideal. Es gibt eine eindeutige Zerlegung von $\mathfrak{p}$ in Maximalideale

$$\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

laut Satz 3.3.15. Daher impliziert Satz 3.4.1, dass

$$\mathsf{N}(\mathfrak{p}) = \mathsf{N}(\mathfrak{p}_1) \cdots \mathsf{N}(\mathfrak{p}_r).$$

Damit die rechte Seite nun eine Primzahl p ist, muss $\mathsf{N}(\mathfrak{p}_i) = 1$ für alle außer genau einen $1 \leq i \leq r$ gelten. Daher muss laut Korollar 3.4.20 $r = 1$ gelten, da ein Maximalideal ungleich (1) ist. Es folgt, dass $\mathfrak{p}$ ein Maximalideal, also ein Primideal, ist. □

Proposition 3.4.27. *Sei $\mathfrak{p} \subseteq \mathfrak{o}_K$ ein Ideal.*

$$\mathfrak{p} \text{ Primideal } \Rightarrow \mathsf{N}(\mathfrak{p}) = p^n, \quad p \text{ Primzahl}$$

für irgendein $1 \leq n \leq r = [K : \mathbb{Q}]$.

Beweis. Jedes Primideal $\mathfrak{p}$ liegt über irgendeine (genau eine) Primzahl $p \in \mathfrak{p} \cap \mathbb{Z}$, sieh unsere Diskussion vor und nach Definition 3.4.24. In anderen Worten $(p) \subseteq \mathfrak{p}$, also $\mathfrak{p} \mid (p)$. Daher implizieren Satz 3.4.1 und Korollar 3.4.17, dass $\mathsf{N}(\mathfrak{p}) \mid \mathsf{N}((p)) = |\mathsf{N}(p)| = p^d$. Die letzte Gleichung ist Lemma 2.2.8.

Das $n \neq 0$ ist klar, da sonst $I = (1)$ folgt (Korollar 3.4.20). □

Definition 3.4.28. Ein Element π eines Ringes R wird *prim* genannt, wenn das Hauptideal $(\pi) \subseteq R$ ein Primideal ist.

Lemma 3.4.29. *Ein Primelement ist immer irreduzibel.*

Beweis. Sei $\pi \in R$ prim und gelte $\pi = xy$. Dann ist $xy \in (\pi)$ und als solches ist o.B.d.A $x \in (\pi)$. Dies wiederum impliziert, dass es ein $a \in R$ gibt, mit $x = a\pi$, woraus wir $\pi = xy = a\pi y$ und daher $1 = ay$ schließen können. Damit ist y eine Einheit, also π irreduzibel. □

Bemerkung 3.4.30. Die Umkehrung stimmt nicht, nicht einmal in Zahlenringen, wie wir es von Proposition 3.4.27 und Beispiel 3.0.8 ablesen können. Im Beispiel ist die Norm nicht die Potenz einer Primzahl, aber wenn (r) ein Primideal wäre, müsste die Norm davon eine Potenz einer Primzahl sein, laut Korollar 3.4.17.

Es gilt aber folgendes:

Proposition 3.4.31. *Sei $\mathfrak{o}_K$ ein Hauptidealring. Ein Element $\pi \in \mathfrak{o}_K$ ist genau dann irreduzibel, wenn $(\pi) \subseteq \mathfrak{o}_K$ ein Primideal ist.*

Beweis. Das prim irreduzibel impliziert ist Lemma 3.4.29. Sei also $(\pi) \subseteq I \subseteq \mathfrak{o}_K$. Laut Korollar 3.3.19 gibt es ein $J \subseteq \mathfrak{o}_K$, so dass $(\pi) = IJ$. Bei Annahme haben wir $I = (x)$ und $J = (y)$, was uns

$$(\pi) = (x)(y) = (xy)$$

gibt. Es ist nun direkt ersichtlich, dass eine Einheit $u \in \mathfrak{o}_K^*$ gibt mit

$$\pi = uxy = x \cdot uy.$$

Da π irreduzibel ist, muss entweder x oder uy eine Einheit sein. Aus $x \in \mathfrak{o}_K^*$ Einheit folgt $(x) = (1)$. Aus $uy \in \mathfrak{o}_K^*$ folgt, dass y eine Einheit ist, also dass $(\pi) = (x)$. Daher ist (π) ein Maximalideal, bzw. Primideal. □

Bemerkung 3.4.32. Der Grund warum wir Proposition 3.4.31 es mit Prim formuliert haben ist, weil die Aussage (mit leichter Modifikation beim Beweis) für Hauptidealbereiche hält. (Es muss also nicht zwingend ein Zahlenring sein. Da sind aber Primideale natürlich nicht mehr maximal).

Proposition 3.4.33. *Ein Element $\pi \in \mathfrak{o}_K$ eines Faktorringes ist genau dann irreduzible, wenn $(\pi) \subseteq \mathfrak{o}_K$ ein Primideal ist.*

Beweis. Auch hier müssen wir nur eine Seite beweisen: Sei $ab \in (\pi)$. Also gibt es ein $c \in \mathfrak{o}_K$, so dass $\pi c = ab$. Wir wollen zeigen, dass $a \in (\pi)$ oder $b \in (\pi)$. Wir können annehmen, dass $a, b, c \neq 0$, da

es sonst trivialerweise erfüllt ist. Satz 3.0.9 besagt, dass es Einheiten $u, v, w \in \mathfrak{o}_K$ und irreduzible Elemente p_i's, q_i's und r_i's gibt, so dass

$$\begin{aligned} a &= up_1 \cdots p_n \\ b &= vq_1 \cdots q_m \\ c &= wr_1 \cdots r_k. \end{aligned}$$

Wir setzen dies ein und erhalten

$$w\pi r_1 \cdots r_k = uvp_1 \cdots p_n q_1 \cdots q_m.$$

Da π irreduzibel und $\mathfrak{o}_K$ bei Annahme ein Faktorring ist, folgt, dass π bis auf Einheit, eines der p_i's oder eines der $q_j's$ ist. Spezifisch teilt π entweder a oder b (oder beides). Daher, $a \in (\pi)$ oder $b \in (\pi)$, also ist (π) ein Primideal. □

Bemerkung 3.4.34. Proposition 3.4.33 ist eine "genau dann" Aussage. Also, $\mathfrak{o}_K$ ist genau dann ein Faktorring, wenn für jedes irreduzible Element $\pi \in \mathfrak{o}_K$, (π) ein Primideal ist. Die andere Seite ist auch nicht viel schwerer zu beweisen.

Aufgaben

Aufgaben 12

Aufgabe 68 (1 Punkt). Sei $\mathcal{B} = \{b_1, \dots, b_d\}$ eine Ganzheitsbasis von $\mathfrak{o}_K$, $0 \neq a \in \mathfrak{o}_K$ und (a) das Hauptideal dazu. Beweise, dass $a\mathcal{B} = \{ab_1, \dots, ab_d\}$ eine Ganzheitsbasis von (a) ist.

Aufgabe 69 (2 Punkte). Sei p eine Primzahl und $\mathfrak{p} \subseteq \mathfrak{o}_K$ ein Primideal. Beweise, dass folgende Aussagen äquivalent sind:

A. $\mathfrak{p} \mid p$, also $\mathfrak{p}$ liegt über p.

B. $p \in \mathfrak{p}$

C. $\mathsf{N}(\mathfrak{p})$ ist eine Potenz von p.

Aufgabe 70 (2 Punkte). Sei $K = \mathbb{Q}(\sqrt{-7})$. Berechne folgende Normen:

i) $\mathsf{N}((11, 2 + \sqrt{-7})^2)$

ii) $\mathsf{N}((8, 1 + \sqrt{-7})^2)$

Aufgabe 71 (3 Punkt). Sei $K = \mathbb{Q}(\sqrt[3]{2})$. Berechne die Norm der Ideale

i) (1 Teilpunkt) $(2, \sqrt[3]{2})$

ii) (1 Teilpunkt) $(3, 1 + \sqrt[3]{2})$

iii) (1 Teilpunkt) $(2, 1 + \sqrt[3]{2})$

Aufgabe 72 (3 Punkte). Sei $[K : \mathbb{Q}] = d$ und sei $\alpha \in \mathfrak{o}_K$ mit $\mathsf{N}(\alpha) = a$.

i) (2 Teilpunkte) Beweise, dass $\mathsf{N}((a, \alpha)^d) = \alpha^d$.

ii) (1 Teilpunkt) Was ist $\mathsf{N}((a, \alpha))$?

Bemerkung 3.4.35. Mit $(A, B) = 1$ meinen wir, dass das schnitt aller Ideale die sowohl A wie auch B enthalten ganz $\mathfrak{o}_K$ ist. Anders gesagt: es gibt $a \in A, b \in B$, so dass $1 = a + b$.

Aufgabe 73 (2 Punkte). Sein $(0) \neq \mathfrak{p}, \mathfrak{q} \subseteq \mathfrak{o}_K$ Primideale mit $\mathfrak{p} \neq \mathfrak{q}$.

i) (1 Teilpunkt) Beweise, dass $(\mathfrak{p}, \mathfrak{q}) = (1)$ und

ii) (1 Teilpunkt) dass $\mathfrak{p} \cap \mathfrak{q} = \mathfrak{p}\mathfrak{q}$.

Aufgabe 74 (2 Punkte). Sein $A, B, C \subseteq \mathfrak{o}_K$ Ideale, so dass $(A, B) = 1$.

i) (1 Teilpunkt) Beweise, dass wenn $A \mid BC$, dann $A \mid C$.

ii) (1 Teilpunkt) Beweise, dass wenn $A \mid C$, $B \mid C$, dann $AB \mid C$.

Aufgabe 75 (3 Punkte). Die Ringe $\mathbb{Z}[\sqrt{6}]$ und $\mathbb{Z}[\sqrt{7}]$ sind Hauptidealringe. (Dies darf man annehmen). Stelle folgende Ideale als Hauptideale dar: (Hinweis: Berechne die Norm der Ideale und finde Elemente β mit der entsprechenden Norm.)

i) (1 Teilpunkt) $(3, \sqrt{6})$,

ii) (1 Teilpunkt) $(5, 4 + \sqrt{6})$,

iii) (1 Teilpunkt) $(2, 1 + \sqrt{7})$.

3.5 Dedekinds Primfaktorzerlegung

Bemerkung 3.5.1. Aus Bemerkung 3.4.25 sehen wir sofort, dass um die Maximalideale von $\mathfrak{o}_K$ zu finden, wir die Hauptideal der Form $(p) \subseteq \mathfrak{o}_K$, für p Primzahl, faktorisieren müssen. Der nächste Satz, was eines der Hauptsätze dieser Vorlesung ist, ermöglicht uns dies.

Das folgende Satz kann etwas allgemeiner formuliert werden, siehe Bemerkung 3.5.5. Es wird Bemerkung genannt, da es in dieser Vorlesung nicht bewiesen wird und nicht zu diesem Kurs gehört.

Satz 3.5.2 (Dedekinds Primfaktorzerlegung)**.** *Sei $\mathfrak{o}_K = \mathbb{Z}[\alpha]$ und $\mathfrak{m}_\alpha \in \mathbb{Z}[X]$ das Minimalpolynom von α. Sei p eine Primzahl und sei*

$$\overline{\mathfrak{m}}_\alpha \equiv \overline{f}_1^{e_1} \cdots \overline{f}_r^{e_r} \mod p,$$

wobei die $\overline{f}_i$'s normiert über $\mathbb{Z}$, irreduzibel über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ sind und $\overline{f}_i = \overline{f}_j \Leftrightarrow i = j$. Das Ideal $(p) \subseteq \mathfrak{o}_k$ faktorisiert als

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

über $\mathfrak{o}_K$, mit

$$\mathfrak{p}_i = (p, f_i(\alpha)),$$

wobei $f_i \in \mathbb{Z}[X]$ eine beliebige Hochhebung von $\overline{f}_i \in \mathbb{F}_p[X]$ ist. Jedes der $\mathfrak{p}_i$ ist maximal, $\mathsf{N}(\mathfrak{p}_i) = p^{\mathsf{grad}(f_i)}$ und $\mathfrak{p}_i = \mathfrak{p}_j \Leftrightarrow i = j$.

Beweis. Die Beweisstrategie ist wie folgt: Als erstes beweisen wir, dass die $\mathfrak{p}_i$'s maximal sind, dann beweisen wir, dass $\prod_{i=1}^n \mathfrak{p}_i^{e_i} \subseteq (p)$ und schließlich, dass die Normen $\mathsf{N}\left(\prod_{i=1}^n \mathfrak{p}_i^{e_i}\right) = \mathsf{N}(p)$ gleich sind. Daraus wird folgen, dass die Ideale miteinander übereinstimmen. Zuletzt beweisen wir noch, dass die $\mathfrak{p}_i$'s alle verscheiden sind.

Die $\mathfrak{p}_i$'s sind maximal: Sei $\mathfrak{p}_i = (p, f_i(\alpha))$, wobei f_i wie in der Aufgabenstellung ist. Wir haben Isomorphien

$$\mathfrak{o}_K/\mathfrak{p}_i \simeq \mathbb{Z}[X]/(\mathfrak{m}_\alpha, p, f_i) \simeq \mathbb{F}_p[X]/(\overline{\mathfrak{m}}_\alpha, \overline{f}_i) \simeq \mathbb{F}_p[X]/(\overline{f}_i), \tag{10}$$

wobei die erste Gleichung von dem Isomorphismus $\varphi : \mathfrak{o}_K \to \mathbb{Z}[X]/\mathfrak{m}_\alpha$ kommt (welches α auf x, und daher $f_i(\alpha)$ auf $f_i = f_i(x)$ sendet) und die Letzte gilt, da $\overline{f}_i$ ein Teiler von $\overline{\mathfrak{m}}_\alpha$ ist. Wir haben auch den Isomorphismus von Proposition 1.1.47 wiederholt angewendet. Da $\overline{f}_i$ irreduzibel bei Annahme ist, folgt aus Proposition 1.3.12, dass $(\overline{f}_i)$ ein Maximal ideal von $\mathbb{F}_p[X]$ ist. Proposition 1.1.49 besagt nun, dass $\mathbb{F}_p[X]/(\overline{f}_i) \simeq \mathfrak{o}_K/\mathfrak{p}_i$ ein Körper-, also $\mathfrak{p}_i$ ein Maximalideal von $\mathfrak{o}_K$ ist.

Es gilt $\prod_{i=1}^n \mathfrak{p}_i^{e_i} \subseteq (p)$: Wir bemerken, dass im Allgemeinen

$$(a, b)(a, c) = (a^2, ac, ab, bc) \subseteq (a, bc)$$

gilt. Daher ist es direkt ersichtlich (leichtes Induktionsargument), dass

$$\prod_{i=1}^n \mathfrak{p}_i^{e_i} = \prod_{i=1}^n (p, f_i(\alpha))^{e_i} \subseteq (p, \prod_{i=1}^n f_i(\alpha)^{e_i}).$$

Auf der anderen Seite haben wir

$$\prod_{i=1}^n f_i(\alpha)^{e_i} \equiv \mathfrak{m}_\alpha(\alpha) \mod p \equiv 0 \mod p$$

bei Annahme. Daher gilt

$$\prod_{i=1}^n f_i(\alpha)^{e_i} \in (p)$$

was uns

$$\prod_{i=1}^{n} \mathfrak{p}_i^{e_i} \subseteq (p)$$

gibt.

Die Normen $\mathsf{N}\left(\prod_{i=1}^{n} \mathfrak{p}_i^{e_i}\right) = \mathsf{N}(p)$ sind gleich: Laut Gleichung (10) ist die Norm $\mathsf{N}(\mathfrak{p}_i) = |\mathfrak{o}_K/\mathfrak{p}_i|$ gleich dem Anzahl der Elemente in $\mathfrak{o}_K/\mathfrak{p}_i = \mathbb{F}_p[X]/(\overline{f}_i)$. Da $\mathbb{F}_p$ ein Körper ist, ist $\mathbb{F}_p/\left(\overline{f}_i\right)$ ein $\mathbb{F}_p$-Vektorraum von Dimension gleich $\mathsf{grad}\left(\overline{f}_i\right)$. Als solches gilt

$$\mathsf{N}(\mathfrak{p}_i) = p^{\mathsf{grad}\left(\overline{f}_i\right)}.$$

Es folgt

$$\begin{aligned}
\mathsf{N}\left(\prod_{i=1}^{n} \mathfrak{p}_i^{e_i}\right) &= \prod_{i=1}^{n} \mathsf{N}(\mathfrak{p}_i)^{e_i} \\
&= \prod_{i=1}^{n} \left(p^{\mathsf{grad}\left(\overline{f}_i\right)}\right)^{e_i} \\
&= \prod_{i=1}^{n} p^{\left(\mathsf{grad}\left(\overline{f}_i\right)\cdot e_i\right)} \\
&= p^{\sum_{i=1}^{n} \mathsf{grad}\left(\overline{f}_i\right)\cdot e_i} \\
&= p^{\mathsf{grad}\left(\prod_{i=1}^{n} \overline{f}_i^{e_i}\right)} \\
&= p^{\mathsf{grad}(\overline{\mathfrak{m}}_\alpha)} \\
&= p^{\mathsf{grad}(\mathfrak{m}_\alpha)} \\
&= p^{[K:\mathbb{Q}]} \\
&= \mathsf{N}((p)).
\end{aligned}$$

Die Gleichung $\mathsf{grad}(\overline{\mathfrak{m}}_\alpha) = \mathsf{grad}(\mathfrak{m}_\alpha)$ gilt, weil $\mathfrak{m}_\alpha$ normiert ist (Minimalpolynom). Daher wird das Leitkoeffizient modulo p nicht 0 werden. Korollar 3.4.21 besagt nun, dass $\prod_{i=1}^{n} \mathfrak{p}_i^{e_i} = (p)$.

Die $\mathfrak{p}_i$'s sind alle verschieden: Sei $(p, f_i(\alpha)) = \mathfrak{p}_i = \mathfrak{p}_j = (p, f_j(\alpha))$. Dann ist $f_j(\alpha) \in \mathfrak{p}_i$, also $\overline{f_j(\alpha)} \equiv 0 \mod \mathfrak{p}_i$. Daher bildet $f_j(\alpha)$ auf 0 in $\mathfrak{o}_k/\mathfrak{p}_i$ ab. Die Isomorphie in Gleichung (10) angewendet besagt, dass f_j auf die Null in $\mathbb{F}_p[X]/(\overline{f}_i)$ abbildet. Daher gilt $\overline{f}_i \mid \overline{f}_j$ in $\mathbb{F}_p[X]$. Da beide normiert und irreduzibel sind, muss $\overline{f}_i = \overline{f}_j$ in $\mathbb{F}_p[X]$ gelten. Bei Annahme haben wir $i = j$, wie gewünscht. □

Mithilfe dieses Satzes können nun beliebige Ideale in Primideale zerlegen. Wie genau dies geht zeigen wir gleich im Algorithmus 3.5.1. Dazu ist es geschickt das Prim- bzw., Maximalideal $(p, f_i(\alpha))$ durch dessen assoziierten (drüber liegenden) Primzahl p zu indexieren, wie wir es in den folgenden Beispielen machen werden, wo wir vorerst die Zerlegung der Ideale der Form $(p) \subseteq \mathfrak{o}_K$ üben.

Beispiel 3.5.3. Sei $K = \mathbb{Q}(\sqrt{6})$. Es gilt $\mathfrak{o}_K = \mathbb{Z}[\sqrt{6}]$ und $\mathfrak{m}_\alpha = x^2 - 6$. Da $\mathfrak{m}_\alpha$ quadratisch ist, ist es genau dann reduzibel, wenn es eine Wurzel hat. Wir setzen einige kleine Zahlen ein um zu sehen, wie $\mathfrak{m}_\alpha$ für einige Primzahlen faktorisiert:

x	x^2-6	Zerlegung modulo $\lvert x^2-6\rvert$	Zerlegung modulo p
0	-6	$x^2 \mod 6$	$x^2 \mod 2$; und $x^2 \mod 3$
± 1	-5	$(x-1)(x+1) \mod 5$	$(x-1)(x+1) \mod 5$
± 2	-2	$(x-2)(x+2) \mod 2$	$x^2 \mod 2$
± 3	3	$(x-3)(x+3) \mod 3$	$x^2 \mod 3$
± 4	10	$(x-4)(x+4) \mod 10$	$x^2 \mod 2$; und $(x+1)(x-1) \mod 5$
± 5	19	$(x-5)(x+5) \mod 19$	$(x-5)(x+5) \mod 19$

Da wir alle Zahlen von -5 bis 5 überprüft haben, wissen wir auch, dass $\mathfrak{m}_\alpha$ irreduzibel ist modulo den Primzahlen bis einschließlich 13 (da $\{-5,\cdots,5\} \equiv \{0,1,5\cdots 10\} \mod n, n \le 11$), die hier nicht vorkommen: also 7 und 11. Wir fassen die verschiedenen Zerlegungen zusammen

$x^2-6 \equiv$	$\mod p$
$\mathbf{x^2}$	$p=2$
$\mathbf{x^2}$	$p=3$
$\mathbf{(x-1)(x+1)}$	$p=5$
x^2-6	$p=7$
x^2-6	$p=11$
?	$p=13$
?	$p=17$
$\mathbf{(x-5)(x+5)}$	$p=19$

wobei wir die reduzierbaren dick schreiben. Wie man sieht, wurden 13 und 17 hier nicht getroffen. Dafür müssten wir noch zusätzlich die Fälle $x=\pm 6$, $x=\pm 7$ und $x=\pm 8$ durchgehen.

Wenn wir nun ein Primideal $(p) \subseteq \mathfrak{o}_K$ zerlegen wollen, sehen wir uns an, wie $\overline{\mathfrak{m}}_\alpha \mod p$ zerfällt: z.B., für (2) haben wir $\overline{x^2+6} = \overline{x}^2$. Also, $r=1$, $f_1 = x$ und $e_i = 2$ in Satz 3.5.2. Wir heben $\overline{x} \in \mathbb{F}_2[X]$ zu $x \in \mathbb{Z}[X]$ hoch (wir könnten auch $x+2 \in \mathbb{Z}[x]$ nehmen etc.) und setzen $\alpha = \sqrt{6}$ ein. Dann erhalten wir

$$(2) = \mathfrak{p}_2^2 = (2, \sqrt{6}).$$

Es ist nun klar, dass auch $(x+2)(\sqrt{6}) = \sqrt{6}+2$ das selbe geliefert hätte, da $(2, \sqrt{6}+2) = (2,\sqrt{6})$. Die Norme der Ideale können wir auch direkt mit dem Satz von Dedekind berechnen. Da der Grad von $\overline{f}_1 = \overline{x} = 1$ ist, haben wir $\mathsf{N}(\mathfrak{p}_2) = 2^1 = 2$.

Wir fassen unsere Zerlegungen in einer Tabelle zusammen:

$(2) = \mathfrak{p}_2^2$	$\mathfrak{p}_2 = (2,\sqrt{6})$	$\mathsf{N}(\mathfrak{p}_2) = 2$
$(3) = \mathfrak{p}_3^2$	$\mathfrak{p}_3 = (3,\sqrt{6})$	$\mathsf{N}(\mathfrak{p}_3) = 3$
$(5) = \mathfrak{p}_5\mathfrak{p}_5'$	$\mathfrak{p}_5 = (5,\sqrt{6}-1),\quad \mathfrak{p}_5' = (5,\sqrt{6}+1)$	$\mathsf{N}(\mathfrak{p}_5) = 5 \quad \mathsf{N}(\mathfrak{p}_5') = 5$
$(7) = \mathfrak{p}_7$	$\mathfrak{p}_7 = (7, 6-6) = (7)$	$\mathsf{N}(\mathfrak{p}_7) = 7^2$
$(11) = \mathfrak{p}_{11}$	$\mathfrak{p}_{11} = (11)$	$\mathsf{N}(\mathfrak{p}_{11}) = 11^2$

Man vergleiche das obige Beispiel mit Aufgabe 60 und das nächste Beispiel mit Aufgabe 62. Sogar in diesen einfachen Fällen sehen wir, wie stark Dedekinds Satz ist.

Beispiel 3.5.4. Sei $K = \mathbb{Q}(\sqrt[3]{2})$. Dann ist $\mathfrak{o}_K = \mathbb{Z}[\sqrt[3]{2}]$ wie in Beispiel 2.4.21 gezeigt. Als solches können wir Dedekinds Primfaktorzerlegungssatz 3.5.2 anwenden. Wir haben $\mathfrak{m}_\alpha = x^3-2$ und wollen $\overline{\mathfrak{m}}_\alpha$ zerlegen. Das zusätzliche Schwierigkeit im kubischen Fall ist, dass wenn wir eine Wurzel $\overline{a}$ gefunden haben, wir die Funktion noch nicht zerlegt haben. Dafür müssen wir erst $\overline{\mathfrak{m}}_\alpha$ mit $\overline{x}-\overline{a}$ teilen und dann das quadratische nochmal zerlegen.

Als Beispiel, $\mathfrak{m}_\alpha(-3) = -29$ in unserem Fall, was eine Primzahl ist. Daher wissen wir, dass $\overline{\mathfrak{m}}_\alpha(-3) \equiv 0 \mod 29$. Also, dass $\overline{x}+\overline{3}$ ein Teiler von $\overline{\mathfrak{m}}_\alpha$ ist, modulo 29. Aber, wir wissen nicht, ob $\overline{x}^3 - \overline{2} : \overline{x}+\overline{3} = \overline{x}^2 - \overline{3x} + \overline{9} \mod 29$ irreduzibel ist modulo 29. Um dies zu überprüfen, müssen wir, a-priori, alle Zahlen von -14 bis 14 in $\overline{x}^2 - \overline{3x} + \overline{9}$ einsetzen und sehen, ob wir Null modulo 29 bekommen. Wir werden eine Zerlegung der kleinen Primzahlen $2, 3, 5$ und 7 geben:

x	x^3-2	Zerlegung $\mod p$
-3	-29	$(x+3)(x^2-3x+9) \mod 29$
-2	-10	$(x+2)(x^2-2x+4) \mod 10 \equiv x^3 \mod 2$ & $(x+2)(x^2-2x+4) \mod 5$
-1	-3	$(x+1)(x^2-x+1) \mod 3$
0	-2	$x^3 \mod 2$
1	-1	1 hat keine Primfaktoren
2	6	$(x-2)(x^2+2x+4) \mod 6 \equiv x^3 \mod 2$ & $(x-2)(x^2+2x+1) \mod 3$
3	25	$(x-3)(x^2+3x+9) \mod 5$

Bei $p = 2$ haben wir die Zerlegung sofort.

Bei $p = 3$ und $p = 5$ haben wir jeweils nur einen der Faktoren gefunden. Da wir aber alle potenziellen Möglichkeiten ($\{-1, 0, 1\}$ für $p = 3$, $\{-2, -1, 0, 1, 2\}$ für $p = 5$) untersucht haben, ist die einzige mögliche Zerlegung von den quadratischen Faktoren eine Wiederholung der Wurzeln: Also, dass $x + 2 \mid x^2 - 2x + 4 \mod 5$ bzw. $x + 1 \mid x^2 - x + 1 \mod 3$. Da $(-2)^2 - 2(-2) + 4 = 12 \not\equiv 0 \mod 5$ ist $x^2 - 2x + 4$ irreduzibel modulo 5. Auf der anderen Seite ist $(-1)^2 - (-1) + 1 = 3 \equiv 0 \mod 3$. Daher ist $x + 1$ ein Teiler von $x^2 - x + 1$ modulo 3. Da, wie schon gesagt, die einzigen potenziellen Wurzeln von $x^3 - 2$ modulo 3 nur $x = -2$ sein kann, wissen wir, dass $x^2 - x + 1 \equiv (x + 2)^3 \mod 3$.

Da 7 kein Teiler von den Werten von $x^3 - 2$ für $-3, \ldots, 3$ ist, wissen wir, dass $x^3 - 2$ irreduzibel ist modulo 7. Wir fassen unsere Diskussion zusammen:

p	Zerlegung von $x^3 - 2$ modulo p
2	$\mathbf{x^3}$
3	$\mathbf{(x+1)^3}$
5	$\mathbf{(x+2)(x^2-2x+4)}$
7	$x^3 - 2$

Daher haben wir folgendes, nach Satz 3.5.2:

$(2) = \mathfrak{p}_2^3$	$\mathfrak{p}_2 = (2, \sqrt[3]{2})$	$\mathsf{N}(\mathfrak{p}_2) = 2$
$(3) = \mathfrak{p}_3^3$	$\mathfrak{p}_3 = (3, \sqrt[3]{2} + 1)$	$\mathsf{N}(\mathfrak{p}_3) = 3$
$(5) = \mathfrak{p}_5\mathfrak{p}_5'$	$\mathfrak{p}_5 = (5, \sqrt[3]{2} + 2), \quad \mathfrak{p}_5' = (5, \sqrt[3]{4} - 2\sqrt[3]{2} + 4)$	$\mathsf{N}(\mathfrak{p}_5) = 5, \quad \mathsf{N}(\mathfrak{p}_5') = 5^2$
$(7) = \mathfrak{p}_7$	$\mathfrak{p}_7 = (7)$	$\mathsf{N}(\mathfrak{p}_7) = 7^3$

Bemerkung 3.5.5 (Allgemeine Form von Dedekinds Primfaktorzerlegung). Sei K ein algebraisches Zahlenkörper und $\alpha \in \mathfrak{o}_K$, so dass $K = \mathbb{Q}(\alpha)$. (So ein α kann man immer finden, Satz 2.1.4 + Lemma 2.3.9). Sei $\mathfrak{m}_\alpha \in \mathbb{Z}[X]$ das Minimalpolynom von α und p eine Primzahl, welches $[\mathfrak{o}_K : \mathbb{Z}[\alpha]]$ *nicht* Teilt, mit

$$\overline{\mathfrak{m}}_\alpha = \overline{f}_1^{e_1} \cdots \overline{f}_n^{e_n} \mod p,$$

wobei die $\overline{f}_i$ normiert und irreduzibel sind über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Dann gilt

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n},$$

wobei die $\mathfrak{p}_i$'s wie in Satz 3.5.2 sind und $\mathfrak{p}_i = \mathfrak{p}_j \Leftrightarrow i = j$. Des weiteren ist $\mathsf{N}(\mathfrak{p}_i) = p^{\mathsf{grad}(\overline{f}_i)}$.

Man bemerke, dass wenn $\mathfrak{o}_K = \mathbb{Z}[\alpha]$, wie in Satz 3.5.2, dann ist $[\mathfrak{o}_K : \mathbb{Z}[\alpha]] = 1$, also gilt die obige Aussage für jeden Primzahl p, da kein Primzahl 1 Teilt.

3.5.1 Algorithmus für die Zerlegung in Maximalideale

Sei $\mathfrak{o}_K = \mathbb{Z}[\alpha]$ und $I \subseteq \mathfrak{o}_K$.

1. Berechne $\mathsf{N}(I) \in \mathbb{Z}$ und faktorisiere es in Primzahlen.
2. Für jeden $p_i \mid \mathsf{N}(I)$, faktorisiere (p_i) in Maximalideale von $\mathfrak{o}_K$, wie in Satz 3.5.2 beschrieben.
3. Liste alle möglichen Produkte dieser Maximalideale, so dass die Norm des Produkts gleich der Norm von I ist.
4. Bestimme, welche dieser Zerlegungen richtig ist.

Bemerkung 3.5.6. Bei Punkt 4 kann man das Produkt der Maximalideale "einfach" ausmultiplizieren und überprüfen, ob es mit (p) übereinstimmt. Wenn man eines gefunden hat, ist man fertig (da alle Produkte verschieden sind). Dies könnte jedoch manchmal etwas knifflig sein. Es gibt viele kleine Tricks mit dem man sich dies vereinfachen kann. Als Beispiel reicht es laut Korollar 3.4.21 aus zu zeigen, dass I ein Unterideal dieses Produkts ist. Wir erinnern uns auch, dass aus $I \subseteq \mathfrak{pq}$ folgt $I \subseteq \mathfrak{p}$ und $I \subseteq \mathfrak{q}$. Die Negation impliziert, dass wenn $I \not\subseteq \mathfrak{p}$, dann $I \not\subseteq \mathfrak{pq}$, was öfters einige Kandidaten ausschließen kann.

Beispiel 3.5.7. Sei $I = (12 + 7\sqrt{6}) \subseteq \mathbb{Z}[\sqrt{6}]$.

1. Dann ist
$$\mathsf{N}(I) = 144 - 6 \cdot 49 = -150 = 2 \cdot 3 \cdot 5^2.$$
2. Von Beispiel 3.5.3 wissen wir, dass die einzigen Primideale mit Norm $2, 3$ oder 5
$$\mathfrak{p}_2 = (2, \sqrt{6}),\ \mathfrak{p}_3 = (3, \sqrt{6}),\ \mathfrak{p}_5 = (5, \sqrt{6} - 1) \quad \text{und} \quad \mathfrak{p}_5' = (5, \sqrt{6} + 1)$$
sind.
3. Daher muss I eines der folgenden Produkte sein:
$$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5^2, \quad \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_5' \quad \text{oder} \quad \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5'^2.$$
4. Als erstes gilt jetzt zu bestimmen, ob $I \subseteq \mathfrak{p}_5$ und ob $I \subseteq \mathfrak{p}_5'$. Da $12 + 7\sqrt{6} = 5 + 7(1 + \sqrt{6})$, ist $I \subseteq \mathfrak{p}_5'$. Daher muss $I \subseteq \mathfrak{p}_5\mathfrak{p}_5'$ oder $I \subseteq \mathfrak{p}_5'^2$ gelten. Wir bemerken, dass $\mathfrak{p}_5\mathfrak{p}_5' = (5)$. Da $12 + 7\sqrt{6}$ offensichtlich kein Vielfaches von 5 ist, folgt $I \nsubseteq \mathfrak{p}_5\mathfrak{p}_5'$. Daher ist
$$I = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5'^2.$$

Bemerkung 3.5.8. Es reicht nicht aus zu zeigen, dass $I \subseteq \mathfrak{p}_i$ für jeden Maximalideal in der Zerlegung. Zum Beispiel, wenn wir zwei Maximalideale $\mathfrak{p}_p, \mathfrak{p}_p'$ der selben Norm $\mathsf{N}(\mathfrak{p}_p) = \mathsf{N}(\mathfrak{p}_p') = p$ haben mit $I \subseteq \mathfrak{p}_p, \mathfrak{p}_p'$ und $\mathsf{N}(I) = p^3$, dann können wir nicht direkt sagen, ob $I = \mathfrak{p}_p\mathfrak{p}_p'^2$ oder $I = \mathfrak{p}_p^2\mathfrak{p}_p'$. Wir müssten noch untersuchen, ob $I \subseteq \mathfrak{p}_p^2$ oder $I \subseteq \mathfrak{p}_p'^2$, oder einen anderen Kriterium zum Unterscheiden finden.

Aufgaben

Aufgaben 13

Aufgabe 76 (3 Punkte). Sei $K = \mathbb{Q}(\sqrt{3})$. Faktorisiere folgende Ideale in $\mathfrak{o}_K = \mathbb{Z}[\sqrt{3}]$ als Produkt von Maximalidealen:

i) (1 Teilpunkt) $(3) \subseteq \mathfrak{o}_K$,

ii) (1 Teilpunkt) $(5) \subseteq \mathfrak{o}_K$,

iii) (1 Teilpunkt) $(7) \subseteq \mathfrak{o}_K$.

Aufgabe 77 (2 Punkte). Sei $K = \mathbb{Q}(\sqrt{-6})$. Faktorisiere $(10) \subseteq \mathfrak{o}_K = \mathbb{Z}[\sqrt{-6}]$ als Produkt von Maximalidealen.

Aufgabe 78 (4 Punkte). Sei $K = \mathbb{Q}(\sqrt[3]{3})$. Faktorisiere folgende Ideale als Produkt von Maximalidealen:

i) (2 Teilpunkte) $(3) \subseteq \mathfrak{o}_K = \mathbb{Z}[\sqrt[3]{3}]$

ii) (2 Teilpunkte) $(10) \subseteq \mathfrak{o}_K = \mathbb{Z}[\sqrt[3]{3}]$

Aufgabe 79 (4 Punkte). Sei $d \not\equiv 1 \mod 4$ eine quadratfreie Zahl und p eine Primzahl, so dass $d \equiv a^2 \mod p$. Sein $\mathfrak{p} := (p, a + \sqrt{d}), \mathfrak{q} := (p, a - \sqrt{d}) \subseteq \mathbb{Z}(\sqrt{d})$.

i) (1 Teilpunkt) Beweise, dass $\mathfrak{p}$ und $\mathfrak{q}$ Primideale sind.

ii) (1 Teilpunkt) Zeige, dass $\mathsf{N}(\mathfrak{p}) = \mathsf{N}(\mathfrak{q}) = p$.

iii) (1 Teilpunkt) Beweise, dass $(p) = \mathfrak{p}\mathfrak{q}$.

iv) (1 Teilpunkt) Zeige, dass $\mathfrak{p} = \mathfrak{q}$ genau dann, wenn $p \mid 2d$.

Sei $f : R \to S$ ein Ringhomomorphismus und $I \subseteq R$ ein Ideal. Dann bezeichnen wir mit I_S, dass Ideal (in S) erzeugt mit $f(I)$. Wenn f eine Einbettung ist, gilt $I_S = (is), i \in I, s \in S$, also das Ideal erzeugt mit allen Produkten is. Folgendes gilt im solchem Fall (was angenommen werden darf):

- $(IJ)_S = I_S J_S$
- $(I^n)_S = (I_S)^n$ und
- $(a)_L = (a)$ (wobei wir a in der rechten Seite als ein Element von S auffassen. Anders gesagt, Hauptideale bleiben Hauptideale und werden vom selben Element erzeugt).

Aufgabe 80 (3 Punkte). Sei $K = \mathbb{Q}(\sqrt{-13})$ und $I = (2, 1 + \sqrt{-13}) \subseteq \mathfrak{o}_K$.

i) (1 Teilpunkt) Beweise, dass $I^2 = (2)$.

ii) (1 Teilpunkt) Zeige, dass I kein Hauptideal ist.

iii) (1 Teilpunkt) Sei $L = \mathbb{Q}(\sqrt{-13}, \sqrt{2})$. Zeige, dass $I_{\mathfrak{o}_L} = (\sqrt{2}) \subseteq \mathfrak{o}_L$. - *Hierzu sagt man, dass man ein Ideal durch eine Erweiterung zu einem Hauptideal gemacht hat.*

Aufgabe 81 (3 Punkte). Sei $d \equiv 1 \mod 4$ und quadratfrei mit $d \neq 1$. Beweise, dass $\mathbb{Z}[\sqrt{d}]$ kein Hauptidealring ist.

Hinweis 1: Faktorisiere $d - 1$. Hinweis 2: Wir haben einen Element $r \in R$ prim genannt, wenn $(p) \subseteq R$ ein Primideal war. Was wissen wir über irreduzible und prim Elemente in einem Hauptidealbereich?

Aufgabe 82 (2 Punkt). Sei $K = \mathbb{Q}(\sqrt{-6})$. Finde alle Ideale der Norm $4, 10$ und 15.

3.6 Idealklassengruppe

Wir haben bewiesen, dass es für algebraische Zahlenringe eine eindeutige Zerlegung von Ideale in Maximalideale gibt, siehe Satz 3.3.15. Diese Ringe haben im allgemeinen jedoch keine eindeutige Zerlegung in irreduzible Elemente, wie im Beispiel 3.0.11 gezeigt. Die Frage bleibt, welche Ringe Faktorringe sind. Um dies und ähnliche Fragen zu studieren, wollen wir eine Invariante genannt *Idealklassengruppe* definieren.

Definition 3.6.1. Ein Bruchideal $I \subseteq K$ heißt *Hauptbruchideal*, wenn es ein Element $a \in K$ gibt, so dass I die Menge der Vielfachen von a ist. - Also $I = \{ab \mid b \in \mathfrak{o}_K\}$.

Lemma 3.6.2. *Ein Hauptbruchideal $I \subseteq K$ ist genau dann ein Hauptideal, wenn $I \subseteq \mathfrak{o}_K$ ein Ideal ist.*

Beweis. Dies ist reine Definition: Sei $I = (r)$ ein Hauptideal, dann ist I ein Ideal und indem man $a = r \in \mathfrak{o}_K \subseteq K$ nimmt, ist es auch ein Hauptbruchideals. Sei $I = \{ab \mid b \in \mathfrak{o}_K\}$ ein Hauptbruchideal, welches sich in $\mathfrak{o}_K$ befindet. Dann muss auch $a = a \cdot 1 \in \mathfrak{o}_K$ sein, also $I = (a)$ als Ideal. Es ist also ein Hauptideal. □

Definition 3.6.3. Sei $\mathcal{I}_K^*$ die Gruppe der Bruchideale von $\mathfrak{o}_K$ ungleich Null und lass $\mathcal{P}_K^*$ die Untergruppe der Hauptbruchidealen von $\mathcal{I}_K^*$ sein. Die *Idealklassengruppe* ist definiert als

$$\mathrm{Cl}(\mathfrak{o}_K) = \mathrm{Cl} = \mathcal{I}_K^*/\mathcal{P}_K^*.$$

Bemerkung 3.6.4. Die Idealklassengruppe, oder sehr nah verwandte Sachen, tauchen öfters mit anderen Namen auf. Es ist ein spezieller Fall der Picardgruppe, welches deutlich allgemeiner für Schematas definiert werden kann, für Zahlenringe stimmen diese aber miteinander überein. Die Anzahl der Elemente der Klassengruppe wird die Klassenzahl, beziehungsweise die Gaußsche Klassenzahl (dies wird jedoch vorallem für den Fall $K = \mathbb{Q}(\sqrt{d})$, mit $d < 0$ benutzt), genannt.

Die Picardgruppe und daher auch die Idealklassengruppe, ist die erste Kohomologiegruppe einer geeigneten Garbe. Das folgende kann man daher als ein kleines Indiz dafür verstehen, dass Garbenkohomologie (auch Grothendieck-Kohomologie genannt) und (Ko-)Homologie im Allgemeinen, von sehr großer Bedeutung in der Mathematik ist.

Satz 3.6.5. *Ein Zahlenring $\mathfrak{o}_K$ ist genau dann ein Faktorring wenn es ein Hauptidealring ist.*

Beweis. Sei $\mathfrak{o}_K$ ein Hauptidealring. Laut Satz 3.0.9 gibt es eine Zerlegung in irreduziblen Elementen. Aus Proposition 3.4.31 wissen wir, dass jedes irreduzible Element $\pi \in \mathfrak{o}_K$ ein Primideal definiert. Satz 3.3.15 impliziert nun Eindeutigkeit.

Sei $\mathfrak{o}_K$ ein Faktorring. Satz 3.3.15 besagt, dass jedes Ideal ein Produkt von Maximalidealen ist. Da das Produkt von Hauptidealen wieder ein Hauptideal ist, brauchen wir nur zu zeigen, dass die Maximalideale mit einem Element erzeugt werden. Sei also $I = \mathfrak{p}$ maximal. Laut Lemma 3.4.19 gibt es eine natürliche Zahl $N = \mathsf{N}(\mathfrak{p}) \in \mathbb{N}$, so dass $N \in \mathfrak{p}$. Daher, $\mathfrak{p} \mid (N)$. Satz 3.0.9 gibt uns eine Zerlegung

$$N = u\pi_1 \cdots \pi_r,$$

mit u Einheit und π's irreduzibel. Da

$$\mathfrak{p} \mid (N) = (u)(\pi_1)\cdots(\pi_r) = (\pi_1)\cdots(\pi_r),$$

impliziert Lemma 1.1.34, dass o. B. d. A., $\mathfrak{p} \mid (\pi_1)$. Da π_1 irreduzibel ist, besagt Proposition 3.4.33, dass (π_1) ein Primideal (bzw. Maximalideal) ist. Wegen Korollar 3.3.19 haben wir $(\pi_1) \subseteq \mathfrak{p}$, also muss $(\pi_1) = \mathfrak{p}$ gelten. Wir haben gezeigt, dass $\mathfrak{p}$ ein Hauptideal ist. □

Lemma 3.6.6. *Sei $(a) = IJ$ ein Hauptbruchideal, so dass I ein Hauptbruchideal ist. Dann ist auch J ein Hauptbruchideal. Das Gleiche gilt auch für Ideale, unter der Annahme, dass alle drei (a), I und J auch Ideale sind.*

Beweis. Aufgabe 83. □

Proposition 3.6.7. *Sei $\mathfrak{o}_K$ ein Zahlenring. Dann ist $\mathrm{Cl}(\mathfrak{o}_K) = 1$, die triviale Gruppe, genau dann wenn $\mathfrak{o}_K$ ist ein Hauptidealring ist. Dies ist äquivalent zu der Aussage, dass $\mathfrak{o}_K$ ein Faktorring ist.*

Beweis. Die Gruppe $\mathrm{Cl}(\mathfrak{o}_K) = \mathcal{I}_K^*/\mathcal{P}_K^*$ ist genau dann trivial, wenn $\mathcal{P}_K^* = \mathcal{I}_K^*$. Also, wenn jedes Bruchideal ein Hauptbruchideal ist.

Sein alle Bruchideale Hauptbruchideale. Spezifisch ist auch jedes Ideal $I \subseteq \mathfrak{o}_K$ ein Hauptbruchideal. Auf der anderen Seite, sein alle Ideale Hauptbruchideale und $I \subseteq K$ ein Bruchideal. Es gibt ein n, so dass $nI \subseteq \mathfrak{o}_K$ ein Ideal, laut Annahme ein Hauptideal und somit ein Hauptbruchideal ist. Da n ein Hauptideal und somit auch ein Hauptbruchideal ist, muss laut Lemma 83 I ein Hauptbruchideal sein.

Da aber ein Hauptbruchideal genau dann ein Hauptideal ist, wenn es ganz in $\mathfrak{o}_K$ liegt, (Lemma 3.6.2), gilt $\mathcal{P}_K^* = \mathcal{I}_K^*$ genau dann wenn jedes Ideal ein Hauptideal ist.

Die Äquivalenz zum Faktorring ist Satz 3.6.5. □

Wir haben gezeigt, dass die Idealklassengruppe genau bestimmt, ob ein Zahlenring ein Faktorring ist. (Obwohl dies nicht mehr Teil des Kurses ist, sollte gesagt werden, dass die Idealklassengruppe misst, *wie weit* ein Zahlenring von einem Faktorring ist. Dies ist aber nicht so einfach wie man meinen könnte.)

Das Problem ist, dass es von der Definition her kaum möglich ist die Idealklassengruppe zu berechnen. Wir wollen nun versuchen diese Gruppe etwas zu studieren.

Satz 3.6.8 (Minkowski-Schranke)**.** *Es gibt eine Konstante $c = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathfrak{o}_K)|}$, welches nur von $\mathfrak{o}_K$ abhängt, so dass für jedes Ideal $0 \neq I \subseteq \mathfrak{o}_K$ ungleich Null, es ein Element $0 \neq x \in I$ gibt, mit*

$$|\mathsf{N}(x)| \leq c\mathsf{N}(I).$$

Was s in der Gleichung ist sagen wir nach Definition 3.6.17. Dieses Lemma wird in Abschnitt 3.7 bewiesen werden. Mithilfe dieser Aussage können wir nun vieles über die Idealklassengruppe beweisen.

Bemerkung 3.6.9. Es gibt auch eine stärkere Version der Konstante c:

$$c = \left(\frac{4}{\pi}\right)^s \frac{d!}{d^d}\sqrt{|\Delta(\mathfrak{o}_K)|},$$

wobei $d = [K : \mathbb{Q}]$ der Grad der Erweiterung ist. Wir werden dies nicht im Kurs beweisen.

Korollar 3.6.10. *Für jedes Ideal $0 \neq I \subseteq \mathfrak{o}_K$ ungleich Null gibt es ein Ideal $J \subseteq \mathfrak{o}_K$, so dass als Elemente der Idealklassengruppe*

- $[J] = [I^{-1}]$ *und*
- $\mathsf{N}(J) \leq c$,

wobei c die Minkowski Konstante ist.

Beweis. Laut Satz 3.6.8 gibt es ein $0 \neq x \in I$, so dass $|\mathsf{N}(x)| \leq c\mathsf{N}(I)$. Korollar 3.3.19 impliziert nun aus $x \in I$, dass es ein $J \subseteq \mathfrak{o}_K$ gibt, mit $IJ = (x)$. Es folgt, dass

$$\mathsf{N}(I)\mathsf{N}(J) = \mathsf{N}(IJ) = \mathsf{N}((x)) = |\mathsf{N}(x)| \leq c\mathsf{N}(I),$$

was nach kürzen mit $\mathsf{N}(I)$, uns $\mathsf{N}(J) \leq c$ gibt. Die Definition der Idealklassengruppe $\mathrm{Cl}(\mathfrak{o}_K) = \mathcal{I}_K^*/\mathcal{P}_K^*$ impliziert von $IJ = (x)$ auch direkt, dass $[IJ] = [(1)]$, also $[J] = [I^{-1}]$. □

Korollar 3.6.11. *Für jeden Bruchideal $I \subseteq K$ gibt es ein Ideal $J \subseteq \mathfrak{o}_K$, so dass*

- $[J] = [I]$ *und*
- $\mathsf{N}(J) \leq c$.

Beweis. Bei Definition eines Bruchideals gibt es ein $n \in \mathbb{N}$, so dass $nI^{-1} \subseteq \mathfrak{o}_K$ ein Ideal ist. Korollar 3.6.10 gibt uns ein Ideal $J \subseteq \mathfrak{o}_K$, mit $\mathsf{N}(J) \leq c$ und $[J] = \left[\left(nI^{-1}\right)^{-1}\right] = \left[\left(I^{-1}\right)^{-1}\right] = [I]$, da $[(n)] = [(1)]$. □

Satz 3.6.12. *Die Gruppe* $\mathrm{Cl}(\mathfrak{o}_K)$ *ist endlich.*

Beweis. Korollar 3.6.11 besagt, dass in jeder Klasse/Orbit/Bahn von Bruchidealen, es ein Ideal mit Norm kleiner als eine fixierte Zahl gibt. Da es nur endlich viele Ideale mit einer gegebenen Norm gibt (und die Norm eine natürliche Zahl ist), siehe Korollar 3.4.22, kann es nur endlich viele Klassen von Bruchidealen geben, denn wenn zwei Klassen/Bahnen ein gemeinsames Element haben, müssen sie gleich sein. - Also, gibt es nur endlich viele Elemente in $\mathrm{Cl}(\mathfrak{o}_K)$. □

Lemma 3.6.13. *Für jedes* $[I] \in \mathrm{Cl}(\mathfrak{o}_K)$ *gibt es ein Ideal* $J \subseteq \mathfrak{o}_K$*, mit* $[I] = [J]$

Bemerkung 3.6.14. Für den Beweis, wie es in der Vorlesung gegeben wurde, sieh Abschnitt .0.3 im Anhang.

Korollar 3.6.15. *Für jedes Ideal* $I \subseteq \mathfrak{o}_K$ *gibt es eine natürliche Zahl* $n \in \mathbb{N}$ *und ein Element* $\alpha \in \mathfrak{o}_K$*, so dass* $I^n = (\alpha)$ *ein Hauptideal ist.*

Beweis. Der Satz von Lagrange (für die Untergruppe $\langle [I] \rangle$) impliziert, dass es einen $n \in \mathbb{N}$ gibt, mit $[I]^n = 1$. Da aber die Einheit der Klassengruppe genau die Klasse der Hauptideale ist, folgt unsere Aussage. □

3.6.1 Methode zum berechnen der Idealklassengruppe

Im Beweis von Satz 3.6.12 haben wir unter anderem folgendes Korollar gezeigt, was uns eine Methode gibt, um die Idealklassengruppe zu berechnen:

Korollar 3.6.16. *Sei* $\mathfrak{o}_K$ *ein algebraischer Zahlenring. Für jeden Element* $[I] \in \mathrm{Cl}(\mathfrak{o}_K) = \mathcal{I}_K^*/\mathcal{P}_K^*$ *(bzw. Klasse in die Quotientengruppe) gibt es ein Ideal* $J \subseteq \mathfrak{o}_K$ *mit* $[I] = [J]$*, so dass*

$$\mathsf{N}(J) \leq c = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathfrak{o}_K)|}.$$

In der obigen Formel ist noch ein unbekanntes für uns, nämlich die Potenz s. Dafür brauchen wir eine Definition:

Definition 3.6.17. Sei K ein Körper und $\sigma : K \to \mathbb{C}$ ein Ringhomomorphismus. Dann heißt σ *reell* wenn $\sigma_i(K) \subseteq \mathbb{R}$ und *komplex* falls nicht.

Eine andere Art und weise dies zu sagen ist, wie folgt: Für eine Einbettung $\sigma : K \to \mathbb{C}$, sei $\overline{(\sigma)}$ die komplex Konjugierte dazu. Formel wird dies Definiert als die Komposition von $\sigma : K \to \mathbb{C}, x \mapsto \sigma(x)$ und $\mathbb{C} \mapsto \mathbb{C}, a + bi \mapsto a - bi$.

Dann gilt $\overline{\overline{\sigma}} = \sigma$ und eine Abbildung $\sigma : K \to \mathbb{C}$ ist genau dann reell wenn $\sigma = \overline{\sigma}$. Es folgt direkt, dass die Anzahl der komplexen Einbettungen gerade ist. Im folgendem Abschnitt 3.7 werden wir sehen, dass die Potenz s in Korollar 3.6.16

$$s = \frac{\text{Anzahl der komplexen Einbettungen}}{2}$$

ist. Wenn r die Anzahl der reellen Einbettungen ist, dann gilt $[K : \mathbb{Q}] =: d = r + 2s$.

Bemerkung 3.6.18. Zum berechnen der Idealklassengruppe gehen wir wie folgt vor:

1. Berechne die Minkowski Schranke c.
2. Betrachte die Ideale mit Norm $\leq c$. Laut Korollar 3.4.22 gibt es nur endlich viele solche Ideale. - Dies besagt, wie viele Elemente es maximal in $\mathrm{Cl}(\mathfrak{o}_K)$ gibt.

– Um die Ideale der Norm $n \in \mathbb{N}$ zu finden, zerlegt man n als das Produkt von Primzahlen $p_1, \dots, p_r$.
– Dann benutzt man Dedekinds Primfaktorzerlegung, Satz 3.5.2 um Maximalideale mit der Norm p_i zu finden.
– Nun nimmt man jedes mögliche Produkt dieser Maximalideale, so dass sie die gewünschte Norm ergeben.

3. Bestimme ob diese Ideale unter dem Quotienten durch $\mathcal{P}_K^*$, den Hauptidealen ungleich Null, gleich werden und finde die Gruppenstruktur von $\mathrm{Cl}(\mathfrak{o}_K)$.
   – Dies ist im allgemeinen der schwerste Schritt und hier gibt es keinen richtigen Algorithmus, sieh Bemerkung 3.6.21, obwohl es natürlich viele Methoden un Tricks gibt.

Wir gehen hier nun einige Beispiel durch.

Beispiel 3.6.19. Sei $K = \mathbb{Q}(i)$ mit $\mathfrak{o}_K = \{1, i\}$. Dann ist $d = 2$, mit $r = 0, s = 1$ und $\Delta(\mathfrak{o}_K) = -4$. Daher haben wir

$$c = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathfrak{o}_K)|} = 2 \cdot \frac{2}{\pi} \approx 1,27.$$

Daher such wie Ideale mit Norm $\leq \lfloor 1,27 \rfloor = 1$. Es gibt nur einen Solchen Ideal, nämlich $(1) = \mathfrak{o}_K$ selbst. Wie in Schritt zwei von 3.6.18 bemerkt gibt es also maximal ein Element in $\mathrm{Cl}(\mathfrak{o}_K)$. Da $1 \in G$ für jede Gruppe, ist $\mathrm{Cl}(\mathfrak{o}_K) = 1$ die triviale Gruppe und somit besagt Satz 3.6.5, dass $\mathbb{Q}(i)$ ein Faktorring ist.

Beispiel 3.6.20. Sei $K = \mathbb{Q}(\sqrt{-6})$. Dann ist $r = 0$, $s = 1$ und $\Delta(\mathfrak{o}_K) = \det \begin{pmatrix} 1 & \sqrt{-6} \\ 1 & -\sqrt{-6} \end{pmatrix}^2 = -24$, was uns

$$c = \frac{2}{\pi}\sqrt{24} \approx 3,11$$

gibt. Daher wissen wir, dass jede Klasse von Bruchidealen in dem Quotient $\mathcal{I}_K^*/\mathcal{P}_K^*$ ein Ideal enthält, mit Norm ≤ 3.

Als solches faktorisieren wir die Ideale $(3) \subseteq \mathfrak{o}_K$ und $(2) \subseteq \mathfrak{o}_K$. Wir benutzen unsere Rechnungen in Beispiel 3.5.3 um zu sagen, dass

$$(2) = (2, \sqrt{-6})^2 = \mathfrak{p}_2$$

und

$$(3) = (3, \sqrt{-6})^2 = \mathfrak{p}_3.$$

Wir habe $\mathsf{N}(\mathfrak{p}_2) = 2$ und $\mathsf{N}(\mathfrak{p}_3) = 3$. Daher gibt es Ideale mit dieser Norm. Es gibt keine weitere Ideale mit Norm 2 oder 3, da sonst $2 \in I$ (bzw. $3 \in I$) gelten würde (Lemma 3.4.19) und als solches, müsste I ein Teiler von (2), (bzw. (3)) sein (Korollar 3.3.19). Da Ideale eindeutig zerfallen (Satz 3.3.15) und wir (2) und (3) schon zerlegt haben, sind diese Tatsächlich die einzigen Ideal mit Norm 2 und 3.

Wir sehen, dass $\mathrm{Cl}(\mathfrak{o}_K)$ ein Quotient der Menge $\{1 = [(1)], [\mathfrak{p}_2], [\mathfrak{p}_3]\}$ ist. Es könnte aber sein, dass noch weitere Elemente gleich gesetzt werden. Zur Erinnerung, die Äquivalenzrelation in $\mathrm{Cl}(\mathfrak{o}_K)$ so gegeben, dass zwei Bruchideale I, J genau dann gleichgesetzt werden, wenn es ein Hauptideal (a) gibt, mit $I = (a)J$.

Wir machen folgende Beobachtungen:

- Da $\mathfrak{p}_2^2 = (2)$ und $\mathfrak{p}_3^2 = (3)$, gilt $[\mathfrak{p}_2]^2 = [\mathfrak{p}_3]^2 = [(1)]$.
  $\Rightarrow$ In einer (der) Gruppe mit 3 Elementen kann dies nicht passieren. Es muss also $[\mathfrak{p}_3] = [(1)]$ oder $[\mathfrak{p}_3] = [\mathfrak{p}_2]$ gelte.

- Wir haben

$$\begin{aligned}\mathfrak{p}_2\mathfrak{p}_3 &= (2,\sqrt{-6})(3,\sqrt{-6})\\ &= (6,2\sqrt{-6},3\sqrt{-6},-6)\\ &= (6,\sqrt{-6})\\ &= (\sqrt{-6})\end{aligned}$$

  $\Rightarrow [\mathfrak{p}_2][\mathfrak{p}_3] = 1.$

- Eine Gruppe ist unter dem Produkt abgeschlossen. In der Menge $\{1 = [(1)], [\mathfrak{p}_2], [\mathfrak{p}_3]\}$ muss es also ein $[\mathfrak{p}_2][\mathfrak{p}_3]$ geben.
  - Aus $[\mathfrak{p}_2][\mathfrak{p}_3] = [\mathfrak{p}_2]$ folgt $[\mathfrak{p}_3] = 1$,
  - aus $[\mathfrak{p}_2][\mathfrak{p}_3] = [\mathfrak{p}_3]$ folgt $[\mathfrak{p}_2] = 1$ und
  - aus $[\mathfrak{p}_2][\mathfrak{p}_3] = 1$ folgt $[\mathfrak{p}_2]^{-1} = [\mathfrak{p}3]$. Wir haben oben schon argumentiert, dass diese Gleichung hält.

In anderen Worten, wir haben mehrere Methoden zu argumentieren, dass $\mathrm{Cl}(\mathfrak{o}_K)$ ein Quotient der Menge $\{1 = [(1)], [\mathfrak{p}_2]\}$ sein muss. Es geht nun also um die Frage, ob $\mathfrak{p}_2 \sim (1)$, also ob $\mathfrak{p}_2$ selber ein Hauptideal ist. Dafür müsste es ein Element $r \in \mathfrak{o}_K$ geben, mit $(r) = \mathfrak{p}_2$, was unter anderem eine Gleichheit der Normen impliziert: Daher

$$2 = \mathsf{N}(\mathfrak{p}_2) = \mathsf{N}((r)) = |\mathsf{N}(r)|.$$

Sei $r = u + v\sqrt{-6}$. Dann ist $\mathsf{N}(r) = u^2 + 6v^2$. Dies kann jedoch nie ± 2 werden, da $u, v \in \mathbb{Z}$ und somit ihre Quadrate positiv sind. Es gibt also ein nicht-trivial Element in $\mathrm{Cl}(\mathfrak{o}_K)$ und daher ist

$$\mathrm{Cl}(\mathfrak{o}_K) = \mathbb{Z}/2\mathbb{Z}.$$

Wir folgern, dass $\mathbb{Q}(\sqrt{-6})$ kein Faktorring ist. Den letzten Teil hätten wir auch von Teil ii) der Aufgabe 59 folgern können.

Bemerkung 3.6.21. Im Allgemeinen ist es nicht einfach, zu sehen, ob ein Ideal I ein Hauptideal ist oder nicht. Sei $I = (x, y) \subseteq \mathfrak{o}_K$ und $\mathcal{B} = \{e_1, \ldots, e_n\}$ ein Ganzheitsbasis von $\mathfrak{o}_K$. Die Frage, ob I ein Hauptideal ist, ist die Frage nach der Existenz von Elementen $u = u_1e_1 + \cdots + u_ne_n$, $a = a_1e_1 + \cdots + a_ne_n$ und $b = b_1e_1 + \cdots + b_ne_n$, so dass

$$ua = x \quad \text{und} \quad ub = y.$$

Dies reduziert sich auf das Lösen von Polynomen vom hohem Grad ($n \times m$ glaube ich, wobei $n = [K : \mathbb{Q}]$ und m die Anzahl der Erzeuger von I ist), was schwer ist!

Zum Beispiel $\mathfrak{o}_K = \mathbb{Z}[\sqrt{d}]$, $I = (x, x)$, mit $x = x_0 + x_1\sqrt{d}$, $y = y_0 + y_1\sqrt{d}$ gibt uns

$$\begin{aligned}(u_0 + u_1\sqrt{d})(a_0 + a_1\sqrt{d}) &= x_0 + x_1\sqrt{d}\\ (u_0 + u_1\sqrt{d})(b_0 + b_1\sqrt{d}) &= y_0 + y_1\sqrt{d}\end{aligned}$$

und somit

$$\begin{aligned}(u_0a_0 + du_1a_1) + (u_0a_1 + u_1a_0)\sqrt{d} &= x_0 + x_1\sqrt{d}\\ (u_0b_0 + du_1b_1) + (u_0b_1 + u_1b_0)\sqrt{d} &= y_0 + y_1\sqrt{d}.\end{aligned}$$

Es geht nun um eine simultane Lösung: Die erste Gleichung gibt uns

$$\begin{aligned}(u_0a_0 + du_1a_1) &= x_0\\ (u_0a_1 + u_1a_0) &= x_1.\end{aligned}$$

Im Allgemeinen muss man nun zuerst den Fall $a_1 = 0$ nehmen und dann $u_0 = \frac{x_1 - u_1 a_0}{a_1}$ schreiben, dies in die Gleichung $(u_0 a_0 + d u_1 a_1) = x_0$ einsetzen und mit a_1 multiplizieren, was uns

$$x_1 a_0 - u_1 a_0^2 + d u_1 a_1^2 = x_0 a_1$$

gibt. Hier sind d und x_0 bekannt, a_0, a_1 und u_1 jedoch nicht. Wir wurden noch eine zweite Gleichung mit den y_i's bekommen, was uns zusammen ein Polynom vom Grad 4 liefern sollte.

Bemerkung 3.6.22. In vielen Fällen kann man sich das Leben deutlich einfacher machen. Eines der Hauptmethoden ist, sich Elemente anzusehen, welche die selbe Norm wie das Ideal I haben. Dann muss man sich noch entscheiden, ob I mit den Hauptidealen übereinstimmt.

Im Fall, we wenn $\mathfrak{o}_K = \mathbb{Z}[\sqrt{d}]$, mit $d < 0$, ist dies recht einfach (zumindest für kleine d), da Elemente mit einer gegebenen Norm immer eine endliche Menge sind. Wir haben es am Beispiel $d = -6$ gesehen.

Wenn $d > 0$, muss man geschickter Vorgehen. Es gibt allgemeine Sätze und Methoden, die man in solchen Fällen benutzen kann (sieh Pellsche Gleichung und Dirichletscher Einheitensatz). In spezifischen Fällen kann man jedoch öfters mit etwas knobeln und argumentieren an eine Lösung kommen.

Z. B., sei $d = 6$, statt -6 und betrachte $I = (2, \sqrt{6})$. Die Frage ist, ob dies ein Hauptideal ist. Wir haben $\mathsf{N}(I) = 2$. Wir wollen also $u, v \in \mathbb{Z}$ finden, mit

$$u^2 - 6v^2 = 2.$$

A priori kann es viele solche u und v geben. In diesem Fall aber können wir zeigen, dass es keine solche gibt: Modulo 3 nämlich haben wir

$$u^2 \equiv -1 \mod 3.$$

Da $0^2 \equiv 0, 1^2 \equiv 1$ und $2^2 \equiv 1$ in $\mathbb{Z}/3\mathbb{Z}$, sehen wir, dass es keinen solchen u geben kann. Daher ist I kein Hauptideal in $\mathbb{Z}[\sqrt{6}]$.

Aufgaben

Aufgaben 14

Aufgabe 83 (1 Punkt). Sei $(a) = IJ$ ein Hauptbruchideal, so dass I ein Hauptbruchideal ist. Beweise, dass auch J ein Hauptbruchideal ist. Beweise das Gleiche auch für Hauptideale, unter der Annahme, dass alle drei (a), I und J auch Ideale sind.

Aufgabe 84 (1 Punkt). Sei $K = \mathbb{Q}(\sqrt{-2})$. Bestimme die Klassgruppe $\mathrm{Cl}(\mathfrak{o}_K)$.

Aufgabe 85 (2 Punkte). Sei $K = \mathbb{Q}(\alpha)$ mit $\mathfrak{o}_K = \mathbb{Z}[\alpha]$, so dass für jede Primzahl $p \leq c$, wobei c die Minkowski Konstante ist, jedes Maximalideal in der Zerlegung von (p) ein Hauptideal ist.

Beweise, dass $\mathrm{Cl}(\mathfrak{o}_K) = 1$ ist. Also, dass K ein Hauptidealring/Faktorring ist.

Aufgabe 86 (2 Punkte). Sei $K = \mathbb{Q}(\sqrt{-10})$. Was ist $\mathrm{Cl}(\mathfrak{o}_K)$?

Aufgabe 87 (1 Punkt). Sei K ein Zahlenkörper und $p \in \mathbb{Z}$ eine Primzahl, so dass $p \nmid \mathrm{Cl}(\mathfrak{o}_K)$. (Also, p teilt die Klassgruppe nicht).

Sei I ein Ideal von $\mathfrak{o}_K$, so dass $I^p = (\theta)$ ein Hauptideal ist. Beweise, dass I ein Hauptideal ist.

Aufgabe 88 (3 Punkte). Sei $K = \mathbb{Q}(\sqrt{-14})$.

i) [1 Teilpunkt] Beweise, dass jede Äquivalenzklasse von Idealen (unter der Äquivalenz $\mathrm{Cl} = \mathcal{I}_K^*/\mathcal{P}_K^*$) einen Ideal der Norm ≤ 4 enthält. Des weiteren zeige, dass $(2) = \mathfrak{p}_2^2 = (2, \sqrt{-14})^2$ und $(3) = \mathfrak{p}_3\mathfrak{q}_3 = (3, 1 + \sqrt{-14})(3, 1 - \sqrt{-14})$.

ii) [1 Teilpunkt] Beweise, dass $(2 - \sqrt{-14}) = \mathfrak{p}_2\mathfrak{p}_3^2$.

iii) [1 Teilpunkt] Schlussfolgere, dass $\mathrm{Cl}(\mathfrak{o}_K)$ die zyklische Gruppe mit 4 Elementen ist.

Aufgabe 89 (4 Punkte). Sei $K = \mathbb{Q}(\sqrt{11})$. Zerlege die Ideale (2), (3) und $(5))$ in Maximalideale. Beweise, dass jedes der Maximalideal die in der Zerlegung von (2), (3) und (5) vorkommen Hauptideale sind. Schlussfolgere, dass $\mathrm{Cl}(\mathfrak{o}_K) = 1$ ist.

Aufgabe 90 (5 Punkte). Sei $K = \mathbb{Q}(\sqrt[3]{5})$. Man darf annehmen, dass $\mathfrak{o}_K = \mathbb{Z}[\sqrt[3]{5}]$ und die verschärfte Konstante

$$c = \left(\frac{4}{\pi}\right)^s \frac{d!}{d^d}\sqrt{|\Delta(\mathfrak{o}_K)|}$$

benutzen, wobei d der Grad der Erweiterung $[K : \mathbb{Q}]$ ist.

i) [1 Teilpunkt] Faktorisiere die Ideale $(2), (3), (5)$ und (7).

ii) [2 Teilpunkte] Beweise, dass alle Maximalideale die in der Faktorisierung von $(2), (3), (5)$ und (7) vorkommen Hauptideale sind und schlussfolgere, dass $\mathrm{Cl}(\mathfrak{o}_K) = 1$ ist.

Ab hier wird nicht abgeprüft.

3.7 Minkowski-Schranke

3.7.1 Gittertheorie und der Minkowskische Gitterpunktsatz

Das Ziel dieses Abschnittes ist es, Satz 3.6.8 (die Minkowski-Schranke) zu beweisen. Dazu brauchen wir einige Definitionen und Lemmas.

Definition 3.7.1. Sei $V \simeq \mathbb{R}^d$ ein $\mathbb{R}$ Vektorraum vom Grad d mit Basis $\mathcal{B} = \{b_1, \ldots, b_d\}$. Wir definieren die *Gitter (bzw. Masche) erzeugt von* $\mathcal{B}$ als

$$L_{\mathcal{B}} = \langle \mathcal{B} \rangle_{\mathbb{Z}} = \langle b_1, \ldots, b_d \rangle_{\mathbb{Z}}$$

und die *Grundmasche* als

$$\mathcal{P} = \left\{ \sum x_i b_i \mid 0 \leq x_i < 1 \right\}.$$

Wie schon von lineare Algebra vertraut gilt

$$\mathrm{Vol}(\mathcal{P}) = |\det(b_1, \ldots, b_d)|. \tag{11}$$

Definition 3.7.2. Eine Teilmenge $U \subseteq V \simeq \mathbb{R}^d$ heißt *konvex* wenn für alle $x, y \in U$ und $\lambda \in [0, 1]$,

$$\lambda x + (1 - \lambda) y \in U$$

gilt.

In anderen Worten, jedes Punkt zwischen x und y in U liegt.

Definition 3.7.3. Eine Teilmenge $U \subseteq V \simeq \mathbb{R}^d$ heißt *symmetrisch*, wenn für jeden $u \in U$, das Gegenpunkt $-u$ auch in U liegt.

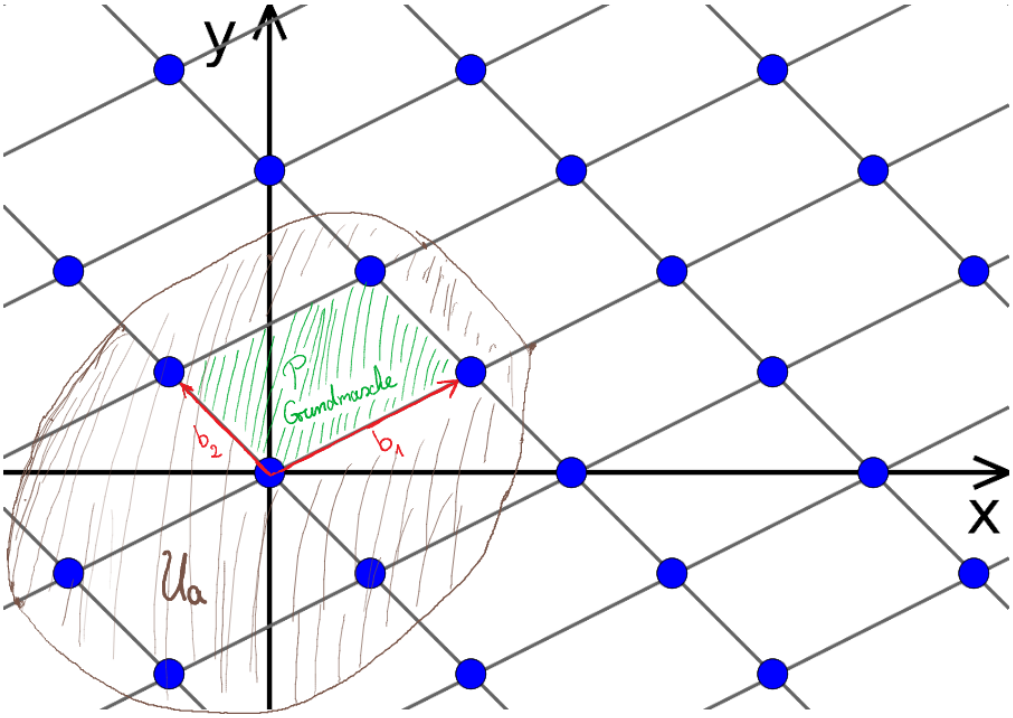
Wir werden das folgende Lemma nicht beweise, da man für einen rigorosen Beweis Maß-Theorie braucht. Dies ist schon bei der Definition $\mathrm{Vol}(U)$ notwendig. In unseren Fällen wird U jedoch einfach genug sein, wo man auch ohne Maß-Theorie eine intuitiv klaren Verständnis von dessen Volumen haben kann.

Eine Beweisskizze davon kann man im Anhang als Satz .0.7 finden.

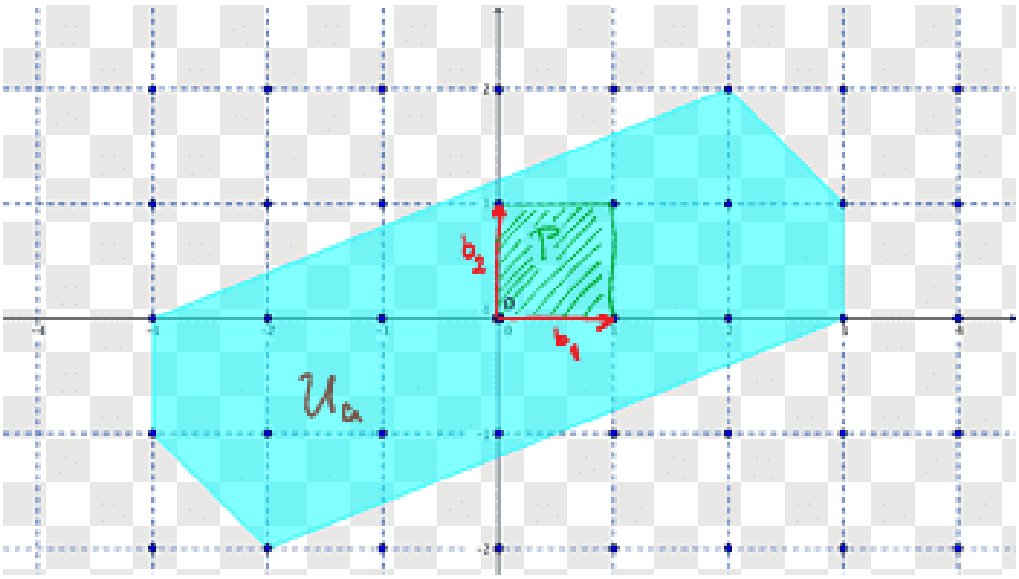
Lemma 3.7.4 (Minkowskischer Gitterpunktsatz)**.** *Sei $U \subseteq V \simeq \mathbb{R}^d$ ein konvexe und symmetrische Teilmenge mit*

$$\mathrm{Vol}(U) > 2^d \mathrm{Vol}(\mathcal{P}),$$

wobei $\mathcal{P}$ die Grundmasche ist. Dann gibt es einen Punkt $0 \neq p \in L$, ungleich Null, von L, dass in U liegt.



Die blauen Punkte sind Elemente von L



Die blauen Punkte sind Elemente von L

3.7.2 Das Lemma von Messy

Eine komplexe Einbettung $\sigma : K \to \mathbb{C}$ hat ein konjugiertes $\overline{\sigma} : K \to \mathbb{C}$, sie unsere Diskussion nach Definition 3.6.17. Als solches definiert das Eine das Andere. Bei reellen Einbettungen ist natürlich $\sigma = \overline{\sigma}$.

Sei $[K : \mathbb{Q}] = d$. Dann gibt es d Verschiedene Einbettungen

$$\sigma_1, \ldots, \sigma_d : K \to \mathbb{C}.$$

Wenn r davon reell sind, dann muss $d-r = 2s$ eine gerade Zahl sein. Wir ordnen diese Einbettungen neu, so dass

- $\sigma_1, \dots, \sigma_r$ reelle Einbettungen sind;
- $\sigma_{r+1}, \dots, \sigma_{r+2s} = \sigma_d$ komplexe sind und
- $\sigma_{r+s+i} = \overline{\sigma}_{r+i}, \quad 1 \le i \le s.$

Definiere das d-dimensionale $\mathbb{R}$-Vektorraum

$$V^{r,s} = \mathbb{R}^r \oplus \mathbb{C}^s.$$

Manchmal wird dies mit K_∞ bezeichnet. Wir definieren die Einbettung

$$\underline{\sigma} : K \to V^{rs}$$

durch

$$\underline{\sigma}(x) = \begin{pmatrix} \sigma_1(x) \\ \vdots \\ \sigma_{r+s}(x) \end{pmatrix}.$$

Achtung, hier werden die Einbettungen $\sigma_{r+s+1}, \dots, \sigma_{r+2s} = \sigma_d$ nicht mit einbezogen. Da $\mathbb{C}$ 2-dimensional ist über $\mathbb{R}$, ist $\dim(V^{r,s}) = d$. Als solches können wir die Frage stellen, ob $\{\underline{\sigma}(b_1), \dots, \underline{\sigma}(b_d)\}$ eine $\mathbb{R}$-Basis von $V^{r,s}$ darstellen, wenn $\{b_1, \dots, b_d\}$ eine $\mathbb{Q}$-Basis von K ist. Die Antwort ist ja und folgendes gilt:

Lemma 3.7.5 (Lemma von Messy)**.** *Sei $\mathcal{B} = \{b_1, \dots, b_d\}$ eine $\mathbb{Q}$-Basis von K. Dann ist $\underline{\sigma}(\mathcal{B}) = \{\underline{\sigma}(b_1), \dots, \underline{\sigma}(b_d)\}$ eine $\mathbb{R}$-Basis von $V^{r,s}$ und es gilt*

$$\mathrm{Vol}(\mathcal{P}) = 2^{-s}\sqrt{|\Delta(\mathcal{B})|}.$$

Die Grundmasche $\mathcal{P}$ ist natürlich bezüglich der Basis $\underline{\sigma}(\mathcal{B})$.

Beweis. Es ist klar, dass

$$\mathrm{Vol}(\mathcal{P}) = |\det(\underline{\sigma}(\mathcal{B}))| = \left| \det \begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & \cdots & \sigma_r(b_d) \\ \mathrm{Re}[\sigma_{r+1}(b_1)] & \cdots & \mathrm{Re}[\sigma_{r+1}(b_d)] \\ \mathrm{Im}[\sigma_{r+1}(b_1)] & \cdots & \mathrm{Im}[\sigma_{r+1}(b_d)] \\ \vdots & & \vdots \\ \mathrm{Re}[\sigma_{r+s}(b_1)] & \cdots & \mathrm{Re}[\sigma_{r+s}(b_d)] \\ \mathrm{Im}[\sigma_{r+s}(b_1)] & \cdots & \mathrm{Im}[\sigma_{r+s}(b_d)] \end{pmatrix} \right|,$$

wie schon in Formel 11 auf Seite 108 gesagt. Hier bezeichnet $\mathrm{Re}(z)$ den reellen Teil einer komplexen Zahl und $\mathrm{Im}(z)$ den imaginären.

Wir fassen die Matrix nun über $\mathbb{C}$ auf. Damit ist diese Gleichung *geometrisch* nicht mehr intuitiv. Algebraisch ist es jedoch klar, da die Determinante über $\mathbb{C}$ und über $\mathbb{R}$ genau gleich ausgerechnet wird.

Indem wir nun die $r + 2a$ Reihen (also die Reihen mit $\mathrm{Im}[\dots]$) mit i multiplizieren und zu den Reihen $r + 2a - 1$ addieren (also den $\mathrm{Re}[\dots]$ die über denen stehen) erhalten wir

$$\mathrm{Vol}(\mathcal{P}) = \left| \det \begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & \cdots & \sigma_r(b_d) \\ \sigma_{r+1}(b_1) & \cdots & \sigma_{r+1}(b_d) \\ \mathrm{Im}[\sigma_{r+1}(b_1)] & \cdots & \mathrm{Im}[\sigma_{r+1}(b_d)] \\ \vdots & & \vdots \\ \sigma_{r+s}(b_1) & \cdots & \sigma_{r+s}(b_d) \\ \mathrm{Im}[\sigma_{r+s}(b_1)] & \cdots & \mathrm{Im}[\sigma_{r+s}(b_d)] \end{pmatrix} \right|.$$

Man multipliziere die Reihen $r+a$ (also wo Im steht) mit $-2i$. Wir erhalten

$$\mathrm{Vol}(\mathcal{P}) = 2^{-s}\left|\det\begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & \cdots & \sigma_r(b_d) \\ \sigma_{r+1}(b_1) & \cdots & \sigma_{r+1}(b_d) \\ -2i\mathrm{Im}[\sigma_{r+1}(b_1)] & \cdots & -2i\mathrm{Im}[\sigma_{r+1}(b_d)] \\ \vdots & & \vdots \\ \sigma_{r+s}(b_1) & \cdots & \sigma_{r+s}(b_d) \\ -2i\mathrm{Im}[\sigma_{r+s}(b_1)] & \cdots & -2i\mathrm{Im}[\sigma_{r+s}(b_d)] \end{pmatrix}\right|.$$

Nun ziehen wir Reihen $r+2a-1$ (also $\sigma_{r+1}, \sigma_{r+3}$, etc.) von den Reihen $r+2a$ (die mit -2Im) ab und erhalten

$$\mathrm{Vol}(\mathcal{P}) = 2^{-s}\left|\det\begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & \cdots & \sigma_r(b_d) \\ \sigma_{r+1}(b_1) & \cdots & \sigma_{r+1}(b_d) \\ \overline{\sigma}_{r+1}(b_1) & \cdots & \overline{\sigma}_{r+1}(b_d) \\ \vdots & & \vdots \\ \sigma_{r+s}(b_1) & \cdots & \sigma_{r+s}(b_d) \\ \overline{\sigma}_{r+s}(b_1) & \cdots & \overline{\sigma}_{r+s}(b_d) \end{pmatrix}\right|.$$

Daher haben wir also alle konjugierten der b_i's erhalten (denn $\overline{\sigma_1}, \ldots \overline{\sigma_r}$ gab uns ja bekanntlich nichts neues) und sonst nichts. Daher ist die Determinante laut Proposition 2.2.12 die Wurzel der Diskriminante von $\mathcal{B}$. Also haben wir

$$\mathrm{Vol}(\mathcal{P}) = 2^{-s}\sqrt{|\Delta(\mathcal{B})|}$$

wie gewünscht.

Nun ist es auch klar, dass $\underline{\sigma}(\mathcal{B})$ genau dann eine $\mathbb{R}$-Basis von $V^{r,s}$ ist, wenn $\mathcal{B}$ eine $\mathbb{Q}$-Basis von K ist, da

$$\det(\underline{\sigma}(\mathcal{B})) = 0 \Leftrightarrow \det(\sigma(\mathcal{B})) = 0.$$

Als solches sind die $\{\underline{\sigma}(b_i)\}$ linear unabhängig. Da

$$\dim_{\mathbb{R}}(V^{r,s}) = \dim_{\mathbb{Q}}(K) = d = r+2s$$

ist $\underline{\sigma}(\mathcal{B})$ eine $\mathbb{R}$-Basis von $V^{r,s}$ und die Aussage ist bewiesen. □

Wir beweisen nun Satz 3.6.8, das wir nochmal aufschreiben:

Satz (Minkowski-Schranke). *Es gibt eine Konstante $c = \left(\frac{2}{\pi}\right)^s\sqrt{|\Delta(\mathfrak{o}_K)|}$, welches nur von $\mathfrak{o}_K$ abhängt, so dass für jedes Ideal $0 \neq I \subseteq \mathfrak{o}_K$ ungleich Null, es ein Element $0 \neq x \in I$ gibt, mit*

$$|\mathsf{N}(x)| \leq \left(\frac{2}{\pi}\right)^s\sqrt{|\Delta(\mathfrak{o}_K)|}\mathsf{N}(I).$$

Beweis. Sei $\mathcal{B}$ eine Ganzheitsbasis von I, also $\mathcal{B}$ ist eine $\mathbb{Q}$-Basis von K und es gilt

$$I = \langle\mathcal{B}\rangle_{\mathbb{Z}}.$$

Die Menge $\underline{\sigma}(I)$ definiert eine Gitter in $\mathbb{R}^d$ mit

$$\mathrm{Vol}(\mathcal{P}) = 2^{-s}|\det(\underline{\sigma}(\mathcal{B}))| = 2^{-s}\sqrt{|\Delta(\mathcal{B})|},$$

wie in Messys Lemma 3.7.5 gezeigt. Sei $\Delta(\mathfrak{o}_K)$ eine Ganzheitsbasis von $\mathfrak{o}_K$. Dann ist laut Proposition 3.4.15

$$\mathsf{N}(I) = \sqrt{\frac{\Delta(\mathcal{B})}{\Delta(\mathfrak{o}_K)}}.$$

Als solches ist

$$\mathrm{Vol}(\mathcal{P}) = 2^{-s}\sqrt{|\Delta(\mathfrak{o}_K)|}\mathsf{N}(I).$$

Sei $a \in \mathbb{R}$ und betrachte folgenden Teilmenge

$$U_a := \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_r \\ x_{r+1} \\ \vdots \\ x_{r+s} \end{pmatrix}, \quad \text{so dass} \quad |x_i| < a \right\} \subseteq V^{r,s} = \mathbb{R}^r \oplus \mathbb{C}^s.$$

Da die einzelnen Koordinate unabhängig von einander sind, ist es das Produkt von r Linien (weil $x_i, 1 \le i \le r$ in $\mathbb{R}$ liegen) und s Kreisflächen (da $x_j, r+1 \le j \le r+s$ in $\mathbb{C}$ sind). Es ist klar, dass U_a symmetrisch und konvex ist, mit Volumen

$$\mathrm{Vol}(U_a) = (2a)^r \left(\pi a^2\right)^s = 2^r \pi^s a^d.$$

Sei $x \in I$. Dann ist $\underline{\sigma}(x) = \begin{pmatrix} \sigma_1(x) \\ \vdots \\ \sigma_{r+s}(x) \end{pmatrix} \in U_a$ für irgendein $a \in \mathbb{R}$. Bei Definition muss dann $|\sigma_i(x)| < a$ für jeden $1 \le i \le r+s$ gelten. Da die Norm eines Elements mit dessen konjugiertem übereinstimmt (Lemma 2.2.2), folgt, dass $|\sigma_i(x)| < a$ für jeden $1 \le i \le d = r + 2s$. Daher gilt

$$\mathsf{N}(x) = \prod_{i=1}^{d} \sigma_i(x) < a^d.$$

Auf der andern Seite können wir den Minkowskischen Gitterpunktsatz 3.7.4 anwenden, wenn $\mathrm{Vol}(U_a) > 2^d \mathrm{Vol}(\mathcal{P})$. Durch Messys Lemma und Formel 12 können wir diese Voraussetzung umformen zu

$$\mathrm{Vol}(U_a) = 2^r \pi^s a^d > 2^d 2^{-s} |\sqrt{\Delta(\mathfrak{o}_K)}|\mathsf{N}(I) = 2^d \mathrm{Vol}(\mathcal{P}).$$

Daher können wir den Minkowskischen Gitterpunktsatz 3.7.4 anwenden, wenn

$$\begin{aligned} & 2^r \pi^s a^d > 2^d 2^{-s} |\sqrt{\Delta(\mathfrak{o}_K)}|\mathsf{N}(I) \\ \Leftrightarrow \quad & a^d > 2^{-r} \pi^{-s} 2^d 2^{-s} |\sqrt{\Delta(\mathfrak{o}_K)}|\mathsf{N}(I) \\ \Leftrightarrow \quad & a^d > 2^s \pi^{-s} |\sqrt{\Delta(\mathfrak{o}_K)}|\mathsf{N}(I) \quad \text{da } d = r + 2s \\ \Leftrightarrow \quad & a^d > c\mathsf{N}(I), \end{aligned}$$

mit

$$c = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathfrak{o}_K)|}.$$

Das heißt, solange a zumindest so groß gewählt ist, ist die Bedingung des Minkowskischen Gitterpunktsatz 3.7.4 erfüllt. Dann gibt es einen Punkt in $\underline{\sigma}(I)$, welches in U_a liegt. Daher, es gibt ein $0 \neq x \in I$, so dass $\underline{\sigma}(x) \in U_a$. Für so einen x haben wir schon gezeigt, dass

$$|\mathsf{N}(x)| < a^d$$

gilt.

Zusammenfassend, wir haben gezeigt, dass es für jeden $n > c\mathsf{N}(I)$, einen $x \in I$ gibt, mit $|\mathsf{N}(x)| < n$. Sei

$$q = \min\{|\mathsf{N}(x)|, \quad \text{mit} \quad x \in I \setminus \{0\}\}.$$

Das Minimum wird natürlich erreicht, da die Norm in $\mathbb{Z}$ ist (Proposition 2.3.14). Es ist klar, dass $q < n$, für jeden $n > c\mathsf{N}(I)$. Daher ist $q \leq c\mathsf{N}(I)$, denn ansonsten wäre $q < q$. Also gibt es einen $0 \neq x \in I$, so dass

$$q = |\mathsf{N}(x)| \leq c\mathsf{N}(I).$$

□

Anhang

Wir wollen hier Lemma 3.7.4 etwas näher begründen. Dies wird kein rigoroser Beweis sein, sondern nur eine grobe Idee geben. Wie schon erwähnt braucht man eigentlich Maßtheorie um dies genau zu beweisen.

Sei $V = \mathbb{R}^d$, $\mathcal{B}$ eine $\mathbb{R}$-Basis von V, $L = \langle \mathcal{B} \rangle_{\mathbb{Z}}$ die dazugehörige Gitter und $\mathcal{P} = \{\sum x_i b_i \mid 0 \leq x < 1\}$ die Grundmasche. Dann ist V die disjunkte Vereinigung von $\mathcal{P}$ mit sich selbst, mal die Anzahl der Elemente in L (was natürlich unendlich ist). Etwas präziser Ausgedrückt, V ist die disjunkte Vereinigung der Parallelverschiebungen durch die Punkte $l \in L$. Als Formel ausgedrückt

$$V = \bigsqcup_{l \in L} (\mathcal{P} + l).$$

Daher kann jedes $v \in V$ eindeutig als $v = p + l$ geschrieben werden, wobei $p \in \mathfrak{p}$ und $l \in L$. Wir definieren die Abbildung (etwas ähnlich zu der Gauß-Abbildung)

$$\pi : V \to \mathcal{P}, \pi(v) = \pi(p + l) = p.$$

Wir haben folgendes:

Lemma .0.6. *Sei $U \subseteq V$ mit $\mathrm{Vol}(U) > \mathrm{Vol}(\mathcal{P})$. Dann gibt es zwei Punkte $v, w \in U$, so dass $v \neq w$ und $v - w \in L$.*

Beweis. Beweis durch Widerspruch. Angenommen, es gibt keine 2 solche Punkte und betrachte die Einschränkung von π auf U, also $\pi|_U : U \to \mathcal{P}$, $u = p + l \mapsto p = u - l$. Sein $u = p + l, u' = p' + l' \in U$, so dass $\pi(u) = \pi(u') \Leftrightarrow p = p'$. Also, $u - l = u' - l'$, woraus $u - u' = l - l'$ folgt. Da $l - l' \in L$, folgt, dass $u - u' \in L$, also muss aus unserer Annahme $u - u'$ folgen, was Injektivität von π impliziert.

Wir schneiden beide Seiten der Gleichung $V = \bigsqcup_{l \in L} (\mathcal{P} + l)$ mit U und erhalten

$$U = \left(\bigsqcup_{l \in L} (\mathcal{P} + l) \right) \cap U = \bigsqcup_{l \in L} U \cap (\mathcal{P} + l) = \bigsqcup_{l \in L} U_l,$$

wobei wir $U \cap (\mathcal{P} + l)$ einfach nur mit U_l bezeichnen. Da $\mathcal{P} + l$ für variierende l disjunkt sind, sind auch die U_l's disjunkt.

Wir behaupten, dass die Mengen $U_l - l$ für verschiedene l disjunkt sind. (Dies ist zu beweisen, da es keine konstante Verschiebung ist, sondern jede der Mengen U_l mit einem anderen $l \in L$ verschoben wird, nämlich ihrem Index). Sei dazu $x \in U_l - l \cap U_k - k$. Dann können wir x schreiben als $x = u - l = v - k$, wobei $u \in U_l$ und $v \in U_k$. Wir wirken mit π auf u und v. Dann ist $\pi(u) = u - l$ und $\pi(v) = v - k$, bei Definition von π. Also solches haben wir $\pi(u) = x = \pi(v)$ was uns $u = v$ aufgrund der Injektivität von π gibt. Aber $u \in U_l$ und $v \in V_k$ - da die U_l's disjunkt sind muss $l = k$ sein, also $U_l - l = U_k - k$. Daher sind die Mengen $U_l - l$ disjunkt.

Nun können wir schreiben

$$\mathrm{Vol}(U) = \sum \mathrm{Vol}(U_l) = \sum \mathrm{Vol}(U_l - l) = \mathrm{Vol}(\bigsqcup (U_l - l)) \leq \mathrm{Vol}(\mathcal{P}),$$

was unser Widerspruch und damit Lemma ergibt.

Wir erklären noch kurz die Gleichungen im obigen Formel: Die erste Gleichung kommt von der Disjunktheit der U_l's. Die zweite von der Tatsache, dass $\mathrm{Vol}(U_l) = \mathrm{Vol}(U_l - l)$, da es eine Verschiebung ist. Die dritte Gleichung gilt weil die $U_l - l$'s immer noch disjunkt sind. Für die vierte Gleichung erinnern wir uns, dass $\pi(v) = v - l$ war, wobei $v = l + p$ war. Daher ist $\pi(U_l) = U_l - l$. Also sind alle $U_l - l$ Teilmengen von $\mathcal{P}$. □

Nun können wir das gewünschte Lemma beweisen:

Lemma .0.7 (Minkowskischer Gitterpunktsatz)**.** *Sei $U \subseteq V \simeq \mathbb{R}^d$ eine konvexe und symmetrische Teilmenge mit*

$$\mathrm{Vol}(U) > 2^d \mathrm{Vol}(\mathcal{P}),$$

wobei $\mathcal{P}$ die Grundmasche ist. Dann gibt es einen Punkt $0 \neq p \in L$, ungleich Null, von L, welches in U liegt.

Beweis. Es gilt $2^d \mathrm{Vol}(\mathcal{P}) = \mathrm{Vol}(2\mathcal{P})$. Daher ist unsere Annahme, dass $\mathrm{Vol}(U) > \mathrm{Vol}(2\mathcal{P})$. Lemma .0.6 besagt, dass es zwei Punkte $u, v \in U$ gibt, mit $u \neq v$ und $u - v \in 2L$, wobei $2L = \langle 2\mathcal{B} \rangle_{\mathbb{Z}}$. Daher ist $(u-v)/2 \in L$ ungleich Null.

Auf der anderen Seite ist $-v \in U$ da U symmetrisch ist. Da es auch konvex ist, muss $(u-v)/2 \in U$ gelten. Damit haben wir also den gewünschten Punkt gefunden. □

.0.3 Vorlesungsversion der Endlichkeit der Idealklassengruppe

Satz .0.8 (Minkowski-Schranke)**.** *Es gibt eine Konstante $c = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathfrak{o}_K)|}$, welches nur von $\mathfrak{o}_K$ abhängt, so dass für jedes Ideal $0 \neq I \subseteq \mathfrak{o}_K$ ungleich Null, es ein Element $0 \neq x \in I$ gibt, mit*

$$|\mathsf{N}(x)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(\mathfrak{o}_K)|} \mathsf{N}(I).$$

Was s in der Gleichung ist sagen wir nach Definition 3.6.17. Dieses Lemma wird in Abschnitt 3.7 bewiesen werden. Mithilfe dieser Aussage können wir nun vieles über die Idealklassengruppe beweisen.

Bemerkung .0.9. Es gibt auch eine stärkere Version der Konstante c:

$$c = \left(\frac{4}{\pi}\right)^s \frac{d!}{d^d} \sqrt{|\Delta(\mathfrak{o}_K)|},$$

wobei $d = [K : \mathbb{Q}]$ der Grad der Erweiterung ist. Wir werden dies nicht im Kurs beweisen.

Satz .0.10. *Die Gruppe $\mathrm{Cl}(\mathfrak{o}_K)$ ist endlich.*

Beweis. Bei Definition haben wir $\mathrm{Cl}(\mathfrak{o}_K) = \mathcal{I}_K^*/\mathcal{P}_K^*$. Sei $I \in \mathcal{I}_K^*$ ein Bruchideal von $\mathfrak{o}_K$. Bei Definition gibt es ein $0 \neq n \in \mathbb{Z}$, so dass $nI \subseteq \mathfrak{o}_K$, also $(n)I$ ein Ideal von $\mathfrak{o}_K$ ist. Da $(n) \in \mathcal{P}_K^*$, bedeutet es, dass $[I] = [(n)I]$ in $\mathrm{Cl}(\mathfrak{o}_K) = \mathcal{I}_K^*/\mathcal{P}_K^*$. Mit $[I]$ meinen wir die Klasse von I in diesem Quotienten. Als solches enthält jede Klasse (bzw. Orbit) in $\mathcal{I}_K^*/\mathcal{P}_K^*$ mindestens einen Ideal.

Sei $J \subseteq \mathfrak{o}_K$ ein Ideal, dass in der Klasse vom Bruchideal $I^{-1} \subseteq K$ liegt. Die Minkowski-Schranke (Satz 3.6.8) besagt, dass es ein $0 \neq x \in J$ gibt, so dass

$$|\mathsf{N}(x)| \leq c\mathsf{N}(J).$$

Da $x \in J$, gilt ja $J \mid (x)$ (Korollar 3.3.19). Daher, es gibt ein $J' \subseteq \mathfrak{o}_K$, mit $JJ' = (x)$. Da $(x) = JJ' \in \mathcal{P}_K^*$ ein Hauptideal ist, gilt $[(x)] = [(1)]$ in Cl. (Denn alles in $\mathcal{P}_K^*$ wird ja zur Einheit in diesem Quotient). Das Quotient ist bekanntlich eine Kongruenzrelation, also mit der Gruppenstruktur verträglich. Wir haben

$$[I] = [I \cdot (1)] = [I(x)] = [IJJ'] = [II^{-1}J'] = [(1)J'] = [J'].$$

Als solches gilt

$$c\mathsf{N}(J) \geq |\mathsf{N}(x)| = \mathsf{N}((x)) = \mathsf{N}(J)\mathsf{N}(J'),$$

was uns

$$\mathsf{N}(J') \leq c$$

gibt. In anderen Worten, in jedem Orbit von $\mathcal{I}_K^*/\mathcal{P}_K^*$ gibt es ein Ideal mit Norm kleiner als eine fixierte Zahl. Da es nur endlich viele Ideale mit einer gegebenen Norm gibt, siehe Korollar 3.4.22, kann es nur endlich viele Klassen von Bruchidealen geben. - Also, nur endlich viele Elemente in $\mathrm{Cl}(\mathfrak{o}_K)$. □

Index

Algebraisch
  Element, 20
Algebraische Zahlen, 41

Dimension
  Vektorraum, 24
Diskriminante, 45

Einbettung
  Komplex, 103
  Reell, 103
Element
  Einheitswurzel, 69
    Primitv, 69
  Ganzalgebraisch, 51
  Prim, 92

Ganzheitsbasis
  Ideal, 89
  Zahlenring, 56
Gitter, 108
Grad
  Koeffizient, 4
  Polynom, 4
Grundmasche, 108
Gruppe
  Abelsch, 3
  Grothendieck, 15
  Homomorphismus, 3

Ideal, 5
  Bruch
    Haupt, 101
  Bruch-, 80
  Endlich erzeugt, 6
  Erzeugt, 5
  Haupt-, 7
  Maximal-, 11
  Prim-, 10, 11
    liegt über, 91
Idealklassengruppe, 101
Integritätsbereich, 4

Konvexe Menge, 108
Körper, 4
  Eisenstein, 67
  Erweiterung, 20
  Kreisteilungs, 69
  Quotienten-, 16
  Teil-, 20
  Unter-, 20
  Zyklotomisch, 69

Leitkoeffizient, 4
Lokalisation, 14

Masche, 108
Modul, 23
  Endlich erzeugt, 24
Module
  Homomorphismus, 24
Moniod
  Unter-, 14
Monoid, 3
  Homomorphismus, 3
  kürzbar, 15
Monomial
  Leit-, 36

Norm
  Element, 44
  Ideal, 77

Ordnung
  Lexikographisch, 36

Polynom
  Konstant, 4
  Minimal-, 21
  Monoisch, 21
  Normiert, 21
  Normiert (kubisch), 62
  Symmetrische, 34
Polynomring, 4
Primitiv, 29

Ring, 3
  Element
    Einheit, 21
    Invertierbar, 21
    Irreduzibel, 21
    Reduzibel, 21
  Euklidisch, 8
  Faktor-, 12
  Faktoriell, 74
  Hauptideal-, 8
  Homomorphismus, 3
  Integritäts-, 4
  Noethersch, 77
  Quotienten-, 12
  Restklassen-, 12

Spur
  Element, 44
Symmetrische Menge, 108

Teiler
Gemeinsamen, 9
Größten gemeinsamen, 9
Teilerfremd, 29

Vektorraum, 24
Basis, 24
Erzeugendes System, 24
Lineare Unabhängigkeit, 24
Endlich dimensional, 24
Homomorphismsus, 24

Zahlenkörper, 41
Kubisch, 61
Quadratisch, 60
Zahlenring, 52

Äquivalenzklasse, 12