Seminarvortrag

Ganze algebraische Zahlen

gehalten von Johannes Hölken
an der Universität Duisburg-Essen im Sommersemester 2012
im Rahmen des Seminars über Elementrare Zahlentheorie.

Kontakt: johannes.hoelken@stud.uni-due.de

Stand: 27. Juni 2012

Betreuung: Philipp Hartwig, Seminarleitung: Prof. Dr. Ulrich Görtz, Philipp Hartwig
Text: A. Schmidt, Einführung in die algebraische Zahlentheorie (Springer Verlag 2007, Berlin-Heidelberg)

Motivation

Bisher haben wir über Eigenschaften von ganzen Zahlen und insbesondere von Primzahlen gesprochen. Im Vortrag über die Gauß'schen Zahlen sahen wir eine erste Verallgemeinerung des Konzepts der ganzen Zahlen und betrachteten zum Beispiel die Primfaktorzerlegung in $\mathbb{Z}[i]$.
Wir wollen nun allgemeinere Ringe der Form $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ mit $\alpha_i \in \mathbb{C}$ untersuchen. Im weiteren Verlauf des Seminars werden uns Zahlen aus solchen Ringen zum Beispiel als „ganze Zahlen" von Kreisteilungskörpern wieder begegnen.

Fassen wir nun die Objekte, die wir in diesem Vortrag untersuchen wollen, genauer mit der ersten

Definition 7.1 *([Ganz] algebraische Zahl)*
Eine komplexe Zahl $\alpha \in \mathbb{C}$ heißt

... *algebraisch über $\mathbb{Q}$, wenn es ein normiertes Polynom*

$$f(X) \;=\; X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \;\in\; \mathbb{Q}[X]$$

mit $f(\alpha) = 0$ gibt.

... *ganz (über $\mathbb{Z}$) oder ganz-algebraisch, wenn es ein normiertes Polynom*

$$f(X) \;=\; X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \;\in\; \mathbb{Z}[X]$$

mit $f(\alpha) = 0$ gibt.

... *transzendent, wenn α nicht algebraisch ist.*

Beispiel 1 *(Algebraische und ganz-algebraische Zahlen)*

- *Jede rationale Zahl $q \in \mathbb{Q}$ ist algebraisch über $\mathbb{Q}$, denn $X - q \in \mathbb{Q}[X]$ ist normiert mit Nullstelle q. Analog ist jede ganze Zahl $z \in \mathbb{Z}$ ganz-algebraisch.*
- *$i \in \mathbb{C}$ ist ganz-algebraisch, denn $X^2 + 1 \in \mathbb{Z}[X]$ ist normiert und hat Nullstelle i.*
- *$\sqrt{2}$ ist ganz-algebraisch, denn $X^2 - 2 \in \mathbb{Z}[X]$ ist normiert und hat Nullstelle $\sqrt{2}$.*

Um zu entscheiden, ob der Begriff „ganz-algebraisch" eine sinvolle Verallgemeinerung von unserem aus $\mathbb{Z} \subset \mathbb{Q}$ bekannten Ganzheitsbegriff ist, müssen wir die Frage stellen, wann eine rationale Zahl ganz algebraisch ist. Die Verallgemeinerung kann nur dann sinnvoll sein, wenn die Begriffe auf $\mathbb{Q}$ übereinstimmen. Und tatsächlich gilt der folgende

Satz 7.2 *Eine rationale Zahl ist genau dann ganz-algebraisch, wenn sie ganz ist.*

Beweis. Wie gesehen ist jede ganze Zahl ganz algebraisch, wir müssen uns also nur um die andere Implikation kümmern. Sei dazu $\alpha \in \mathbb{Q} \setminus \mathbb{Z}$, dann gibt es $p \in \mathbb{Z}$ und $q \in \mathbb{N}$[1] mit $\alpha = \frac{p}{q}$. Insbesondere können wir ohne Einschränkung p und q so wählen, dass p und q Teilerfremd sind (sonst kürze den Bruch). Angenommen es gäbe ein normiertes Polynom

$$f(X) \;=\; X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \;\in\; \mathbb{Z}[X]$$

[1] Beachte $\mathbb{N} \neq \mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

mit $f(\alpha) = 0$, dann erhielten wir durch Multiplizieren mit q^n

$$\begin{aligned} f(q) \;=\; 0 \;\;&\Leftrightarrow\;\; \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\left(\frac{p}{q}\right) + a_0 \;=\; 0 \\ &\Leftrightarrow\;\; p^n + p^{n-1}qa_{n_1} + \ldots + pq^{n-1}a_1 + q^n a_0 \;=\; 0 \end{aligned}$$

also wäre p^n durch q teilbar. Das ist ein Widerspruch zur Teilerfremdheit von p und q. □

Folgerung 7.3 *$\sqrt{2}$ ist irrational.*

Beweis. Wir haben bereits gesehen, dass $\sqrt{2}$ ganz-algebraisch ist. Angenommen $\sqrt{2}$ wäre eine rationale Zahl, dann wäre $\sqrt{2} \in \mathbb{Z}$ nach Satz 7.2. Das ist offensichtlich falsch. □

Wir wollen den Zusammenhang von algebraischen und ganz-algebraischen Zahlen noch genauer studieren. Wir wissen, dass es für jede rationale zahl $\alpha \in \mathbb{Q}$ eine natürliche Zahl $n \in \mathbb{N}$ gibt, so dass $nq \in \mathbb{Z}$ ist. Heraus erhalten wir die folgende Charakterisierung

Lemma 7.4 *Eine komplexe Zahl $\alpha \in \mathbb{C}$ ist genau dann algebraisch, wenn es eine natürliche Zahl $m \in \mathbb{N}$ so gibt, dass $m\alpha$ ganz-algebraisch ist.*

Beweis. Sei $\alpha \in \mathbb{C}$ algebraisch, dann gibt es ein Polynom

$$f(X) \;=\; X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \;\in\; \mathbb{Q}[X]$$

mit $f(\alpha) = 0$. Wähle nun eine natürliche Zahl $m \in \mathbb{N}$ groß genug, so dass $ma_i \in \mathbb{Z}$ für alle $i = 0, \ldots, n-1$ gilt. Damit gilt

$$(m\alpha)^n + m\,a_{n-1}\,(m\alpha)^{n-1} + \ldots + m^n\,a_0 \;=\; 0$$

wir haben also ein normiertes Polynom mit ganzzahligen Koeffizienten und Nullstelle $m\alpha$ gefunden. Dass heißt aber gerade, dass $m\alpha$ ganz algebraisch ist. Der Umgekehrte Schluss zeigt, dass aus $m\alpha$ ist ganz-algebraisch stets folgt, dass α algebraisch ist. □

Definition und Lemma 7.5 *Sei $n \in \mathbb{N}$. Für das n-Tupel natürlicher Zahlen $i = (i_1, \ldots, i_n)$ setzen wir $|i| := i_1 + \ldots + i_n$ sowie die Kurzschreibweisen*

$$a_i \;:=\; a_{i_1,\ldots,i_n} \quad \text{und} \quad \underline{X}^i \;:=\; X_1^{i_1} \cdots X_n^{i_n}$$

Seien $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ komplexe Zahlen, dann setzen wir

$$\mathbb{Z}[\alpha_1, \ldots, \alpha_n] \;:=\; \left\{ \sum_{|i|=0}^{d} a_i\,\underline{\alpha}^i \;\middle|\; d \in \mathbb{N} \wedge a_i \in \mathbb{Z} \right\}$$

und sagen $\mathbb{Z}$ adjungiert $\alpha_1, \ldots, \alpha_n$. Die Menge $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ ist ein Ring.

Beweis. Betrachte den Evaluationshomomorphismus

$$\begin{aligned} ev : \mathbb{Z}[X_1, \ldots, X_n] &\to \mathbb{C} \\ X_i &\mapsto \alpha_i \end{aligned}$$

Nach dem Homomorphiesatz ist $\mathrm{Im}(ev) \subset \mathbb{C}$ ein Unterring.

Behauptung $\mathrm{Im}(ev) = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$

Die Inklusion „$\subseteq$“ ist klar. Für die andere Richtung sei

$$f \;=\; \sum_{|i|=0}^{d} a_i \, \underline{\alpha}^i \;\in\; \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$$

dann ist

$$\tilde{f} \;:=\; \sum_{|i|=0}^{d} a_i \, \underline{X}^i \;\in\; \mathbb{Z}[X_1, \ldots, X_n]$$

ein Urbild von f unter ev, damit ist $f \in \mathrm{Im}(ev)$. □

Beispiel 2 *Wir kennen bereits den Ring der Gaußschen Zahlen* $\mathbb{Z}[i] = \{\, a + ib \,|\, a, b \in \mathbb{Z} \,\}$. *Es gilt*

$$\begin{aligned} \sum_{n=0}^{d} a_n i^n &= \sum_{\substack{n=0 \\ 2|n}}^{d} a_n \big(i^2\big)^{\frac{n}{2}} + \sum_{\substack{n=1 \\ 2\nmid n}}^{d} a_n i \, \big(i^2\big)^{\frac{n-1}{2}} \\ &= \underbrace{\sum_{\substack{n=0 \\ 2|n}}^{d} a_n \big(-1\big)^{\frac{n}{2}}}_{\in \mathbb{Z}} + i \cdot \underbrace{\sum_{\substack{n=1 \\ 2\nmid n}}^{d} a_n \big(-1\big)^{\frac{n-1}{2}}}_{\in \mathbb{Z}} \end{aligned}$$

Damit passt unsere Definition tatsächlich auf den bekannten Ring $\mathbb{Z}[i]$.

Das im Beispiel entdeckte Phänomen gilt noch allgemeiner. Dies zeigt der folgende

Satz 7.6 *Seien* $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$*, dann gilt:* $(\mathbb{Z}[\alpha_1, \ldots, \alpha_n], +)$ *ist genau dann eine endlich erzeugte abelsche Gruppe, wenn* $\alpha_1, \ldots, \alpha_n$ *ganz-algebraisch sind.*

Beweis. Seien $\alpha_1, \ldots, \alpha_n$ ganz-algebraisch, dann gibt es für $i = 1, \ldots, n$ normierte Polynome

$$f_i(X) \;=\; X^{d_i} + \sum_{j=0}^{d_i - 1} a_{i,j} \, X^j \;\in \mathbb{Z}[X]$$

mit $f_i(\alpha_i) = 0$. Es gilt

$$\begin{aligned} f_i(\alpha_i) \;=\; 0 \;\;&\Leftrightarrow\;\; \alpha_i^{d_i} + \sum_{j=0}^{d_i - 1} a_{i,j} \, \alpha_i^j \;=\; 0 \\ &\Leftrightarrow\;\; \alpha_i^{d_i} \;=\; -\sum_{j=0}^{d_i - 1} a_{i,j} \, \alpha_i^j \end{aligned}$$

für alle $i = 1, \ldots, n$. Wir können also erreichen, dass in den beliebigen endlichen Summen, von denen $\mathbb{Z}[\alpha_i, \ldots, \alpha_n]$ nach Definition 7.5 erzeugt wird, jedes α_i höchstens in der Potenz $d_i - 1$ vorkommt. Dann ist aber $\mathbb{Z}[\alpha_i, \ldots, \alpha_n]$ als abelsche Gruppe bereits von den Elementen

$$\left\{ \alpha_1^{e_1} \cdots \alpha_n^{e_n} \,\middle|\, 0 \leq e_i \leq d_i - 1 \right\}$$

erzeugt.
Sei nun $(\mathbb{Z}[\alpha_1, \ldots, \alpha_n], +)$ endlich erzeugt. Für alle $j = 1, \ldots, n$ ist auch

$$\mathbb{Z}[\alpha_j] \;\subset\; \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$$

endlich erzeugt, denn aus dem letzten Vortrag wissen wir: Jede Untergruppe einer endlich erzeugten abelschen Gruppe ist selbst endlich erzeugt. Wähle nun ein $\alpha := \alpha_j$ fest aus, dann gibt es ein endliches Erzeugendensystem

$$\mathcal{E} \;=\; \left\{ \sum_{i=0}^{d_j} a_{i,j}\alpha^i \,\middle|\, d_j \in \mathbb{N} \wedge j = 1 \ldots N \right\} \;\subset\; \mathbb{Z}[\alpha]$$

Setze nun $n := \max\{d_1, \ldots, d_N\}$. Dann ist auch

$$\mathcal{E}' \;=\; \left\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right\}$$

ein Erzeugendensystem von $\mathbb{Z}[\alpha]$, also gibt es ganze Zahlen $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ mit

$$\alpha^n = -a_{n-1}\,\alpha^{n-1} - \ldots - a_1\alpha - a_0 \;\;\Leftrightarrow\;\; 0 = \alpha^n + a_{n-1}\,\alpha^{n-1} + \ldots + a_1\alpha + a_0$$

Dann ist aber $f(X) = X^n + a_{n-1}\,X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$ ein normiertes Polynom mit Nullstelle α und damit ist α ganz-algebraisch. □

Definition und Folgerung 7.7 *(Ring der ganz-algebraischen und Körper der algebraischen Zahlen)*

(i) *Die Menge der ganz-algebraischen Zahlen $\mathcal{O} \subset \mathbb{C}$ über $\mathbb{Z}$ ist ein Ring.*

(ii) *Die Menge der algebraischen Zahlen $\overline{\mathbb{Q}} \subset \mathbb{C}$ über $\mathbb{Q}$ ist ein Körper.*

Beweis. Für Teil **(i)** müssen wir zeigen, dass je die Summe und das Produkt zweier ganz-algebraischen Zahlen wieder eine ganz-algebraische Zahl ist. Seien also $\alpha, \beta \in \mathcal{O}$ ganz-algebraisch, dann ist $\mathbb{Z}[\alpha, \beta]$ nach Satz 7.6 endlich erzeugt. Da $\mathbb{Z}[\alpha, \beta]$ nach Lemma 7.5 ein Ring ist gilt $\alpha + \beta \in \mathbb{Z}[\alpha, \beta]$. Damit ist $\mathbb{Z}[\alpha + \beta]$ als Untergruppe der endlich erzeugten abelschen Gruppe $\mathbb{Z}[\alpha, \beta]$ endlich erzeugt. Nach Satz 7.6 ist $\alpha + \beta$ dann ganz-algebraisch. Der Nachweis für das Produkt zweier ganzer Zahlen erfolgt ganz analog.
Für Teil **(ii)** müssen wir nicht nur, wie oben, zeigen, dass Produkt und Summe zweier algebraischer Zahlen wieder algebraisch sind, sondern auch, dass das Inverse einer algebraischen Zahl ungleichh Null wieder eine algebraische Zahl ist. Seien nun $\alpha, \beta \in \overline{\mathbb{Q}}$ algebraisch, dann gibt es nach Lemma 7.4 natürliche Zahlen $a, b \in \mathbb{N}$ so dass $a\alpha$ und $b\beta$ ganz-algebraisch sind. Natürlich sind dann auch $ab\alpha$ und $ab\beta$ ganz-algebraisch. Nach Teil **(i)** sind dann $ab\alpha + ab\beta = ab(\alpha + \beta)$ und $a\alpha \cdot b\beta = ab(\alpha\beta)$ ganz-algebraisch. Mit Lemma 7.4 sind damit $\alpha + \beta$ und $\alpha\beta$ algebraisch.
Sei nun $\alpha \in \overline{\mathbb{Q}}\backslash\{0\}$, dann gibt es ein normiertes Polynom

$$f(X) \;=\; X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \;\in\; \mathbb{Q}[X]$$

mit $f(\alpha) = 0$. Ohne Einschränkung sei $a_0 \neq 0$ (sonst teile genügend oft durch X). Dann gilt

$$\frac{f(\alpha)}{a_o\,\alpha^n} \;=\; 0 \;\;\Leftrightarrow\;\; \underbrace{\frac{1}{a_0}}_{=:\,b_0} + \underbrace{\frac{a_{n-1}}{a_0}}_{=:\,b_1}\cdot\Big(\frac{1}{\alpha}\Big) + \ldots + \Big(\frac{1}{\alpha}\Big)^n \;=\; 0$$

und

$$g(X) \;:=\; X^n + b_{n-1}X^{n-1} + \ldots + b_1X + b_0 \;\in\; \mathbb{Q}[X]$$

ist ein normiertes Polynom mit $g(\frac{1}{\alpha}) = 0$ also ist $\frac{1}{\alpha}$ algebraisch. □

Anmerkung Es gibt kein Polynom $f \in \mathbb{Q}[X]$ mit $f(\pi) = 0$, also ist π transzendent. Wegen $\pi \in \mathbb{C}$ und $\sqrt{2} \notin \mathbb{Q}$ sind die Inklusionen

$$\mathbb{Q} \;\subsetneq\; \overline{\mathbb{Q}} \;\subsetneq\; \mathbb{C}$$

echt.

Definition und Satz 7.8 *Sei $\alpha \in \mathbb{C}$. Es gelten*

- *Ist α Nullstelle eines normierten Polynoms $f \in \mathcal{O}[X]$, so ist $\alpha \in \mathcal{O}$*
- *Ist α Nullstelle eines normierten Polynoms $f \in \overline{\mathbb{Q}}[X]$, so ist $\alpha \in \overline{\mathbb{Q}}$*

Wir sagen $\mathcal{O}$ ist ganz abgeschlossen und $\overline{\mathbb{Q}}$ ist algebraisch abgeschlossen.

Beweis. Sei α eine Nullstelle von

$$f(X) \;=\; X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \;\in\; \mathcal{O}[X]$$

dann ist $\mathbb{Z}[\alpha, a_0, \ldots, a_{n-1}]$ als abelsche Gruppe endlich erzeugt, denn wegen

$$f(\alpha) \;=\; 0 \;\;\Leftrightarrow\;\; \alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha - a_0$$

können wir die gleiche Argumentation wie im Beweis von Satz 7.6 anwenden. Aus eben diesem Satz folgt dann auch die Behauptung.
Sei nun α eine Nullstelle von

$$f(X) \;=\; X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \;\in\; \overline{\mathbb{Q}}[X]$$

Dann gibt es nach Lemma 7.4 natürliche Zahlen $m_i \in \mathbb{N}$ so dass $m_i \cdot a_i \in \mathcal{O}$ für alle $i = 0, \ldots, n-1$. Setze $m := \max\{m_i | i = 0, \ldots, n-1\}$, dann ist $mf \in \mathcal{O}[X]$ und

$$\begin{aligned} mf(\alpha) &= m\alpha^n + ma_{n-1}\alpha^{n-1} + \ldots + ma_1\alpha + ma_0 \\ &= 0 \end{aligned}$$

aber das Polynom mf ist nicht normiert. Betrachte daher $m^nf \in \mathcal{O}[X]$, dann gilt

$$\begin{aligned} 0 \;=\; m^nf(\alpha) &= m^n\alpha^n + m^na_{n-1}\alpha^{n-1} + \ldots + m^na_1\alpha + m^na_0 \\ &= (m\alpha)^n + ma_{n-1}(m\alpha)^{n-1} + \ldots + m^{n-1}a_1\,(m\alpha) + m^na_0 \end{aligned}$$

also ist $m\alpha$ Nullstelle eines normierten Polynoms mit ganz-algebraischen Koeffizienten, also nach dem bereits bekannten Teil selbst ganz-algebraisch. Schließlich ist α nach Lemma 7.4 algebraisch. □

Definition 7.9 *(Minimalpolynom von α)*
Sei $\alpha \in \mathbb{C}$ algebraisch über $\mathbb{Q}$. Ein Polynom $f_\alpha \in \mathbb{Q}[X]$ heißt Minimalpolynom von α, falls die folgenden Bedingungen gelten:

(1) *f_α ist normiert, das heißt der höchste Koeffizient ist* 1.

(2) *α ist eine Nullstelle von f_α, also $f_\alpha(\alpha) = 0$.*

(3) *Für alle $f \in \mathbb{Q}[X]$ die die Eigenschaft **(2)** erfüllen gilt* $\deg(f_\alpha) \leq \deg(f)$.

Anmerkung Nach dieser Definition ist sofort klar, dass zu jedem α mindestens ein Minimalpolynom f_α existiert, denn α ist genau dann algebraisch, wenn ein Polynom existiert, dass die Bedingungen **(1)** und **(2)** erfüllt. Genaueres über Minimalpolynome zeigt der nächste

Satz 7.10 *Sei $\alpha \in \mathbb{C}$ algebraisch über $\mathbb{Q}$, dann gelten*

(i) *Das Minimalpolynom f_α von α ist eindeutig bestimmt.*

(ii) *Das Minimalpolynom f_α von α ist irreduzibel.*

(iii) *Das Minimalpolynom f_α von α teilt jedes Polynom $g \in \mathbb{Q}[X]$ mit $g(\alpha) = 0$.*

Beweis. Seien $f_\alpha \in \mathbb{Q}[X]$ ein Minimalpolynom von α und $g \in \mathbb{Q}[X]$ ein weiteres Polynom, dass die Eigenschaft $g(\alpha) = 0$ erfüllt. Sei weiter $h \in \mathbb{Q}[X]$ ein größter gemeinsamer Teiler von f_α und g. Dann gibt es $\varphi, \psi \in \mathbb{Q}[X]$ mit $h = \varphi f_\alpha + \psi g$ also ist

$$h(\alpha) \;=\; \varphi(\alpha) \cdot f_\alpha(\alpha) + \psi(\alpha) \cdot g(\alpha) \;=\; 0$$

Nach Voraussetzung hat f_α unter allen Polynomen, die α als Nullstelle haben, minimalen Grad. Damit gibt es ein $q \in \mathbb{Q}$ mit $f = qh$, also $f \hat{=} h$.
Da g ein beliebiges Polynom mit der Eigenschaft $g(\alpha) = 0$ war, ist f_α ein größter gemeinsamer Teiler von allen Polynomen mit dieser Eigenschaft, also folgt Teil **(iii)**.
Für die erste Aussage nimm an, dass auch g normiert sei und minimalen Grad habe, dann gilt

$$f \hat{=} h \hat{=} g$$

Es gibt also ein $q' \in \mathbb{Q}$, so dass $f = qg$ aber der höchste Koeffizient von Beiden Polynomen ist 1, also müssen die Polynome gleich sein.
Für den Nachweis von **(ii)** nimm an, dass f_α nicht irreduzibel sei. Dann gäbe es Polynome $k, r \in \mathbb{Q}[X]$ mit $\deg(k), \deg(r) > 0$ und $f_\alpha = k \cdot r$. Da aber α eine Nullstelle des Minimalpolynoms f_α ist, müsste auch $k(\alpha) = 0$ oder $r(\alpha) = 0$ gelten. Dies Widerspräche aber der Bedingung, dass f minimalen Grad unter allen Polynomen mit dieser Eigenschaft haben soll. □

Abschließend wollen wir überlegen, was wir über Minimalpolynomen von ganz-algebraischen Zahlen sagen können. Dafür benötigen wir zunächst ein allgemeineres Ergebnis:

Lemma 7.11 *Sei $f \in \mathbb{Z}[X]$ ein normiertes Polynom. Sei*

$$f = p_1 \cdots p_n$$

seine Zerlegung in nicht notwendig verschiedene aber normierte Primpolynome aus $\mathbb{Q}[X]$. Dann haben alle Primpolynome p_i bereits ganzzahlige Koeffizienten, liegen also in $\mathbb{Z}[X]$.

Beweis. Wir zeigen zunächst eine noch allgemeinere Aussage

Behauptung *Seien $f, g \in \mathbb{Q}[X]$ normierte Polynome. Gilt $fg \in \mathbb{Z}[X]$ so sind bereits $f, g \in \mathbb{Z}[X]$.*
Beweis. Seien

$$f(X) \;=\; X^n + \sum_{i=0}^{n-1} a_i\, X^i \quad \text{und} \quad g(X) \;=\; X^m + \sum_{i=0}^{m-1} b_i\, X^i$$

Seien nun $M, N \in \mathbb{N}$ die kleinste Natürliche Zahl, mit der Eigenschaft $Nf, Mg \in \mathbb{Z}[X]$, dann setze

$$A_i \;:=\; N \cdot a_i \quad \text{für alle } i = 0, \ldots, n-1$$

und B_j analog. Es gilt

$$MNfg \;=\; A_n B_n\, X^{n+m} + (A_n B_{m-1} + A_{n-1} B_m) X^{n+m-1} + \ldots + A_0 B_0$$

Nach Voraussetzung ist $fg \in \mathbb{Z}[X]$, also sind alle Koeffizienten auf der linken, und damit auch auf der rechten Seite, der Gleichung durch NM teilbar. Angenommen $NM > 1$, dann gibt es eine Primzahl $p \in \mathbb{Z}$, die MN teilt. Da p eine Primzahl ist, ist

$$\mathbb{Z}\!\diagup_{p\,\mathbb{Z}}[X] \;=\; \mathbb{F}_p[X]$$

ein Polynomring über einem Körper und als solcher Nullteilerfrei. Da MN von p geteilt wird, ist

$$\overline{(Nf)}\;\overline{(Mg)} \;=\; \overline{(Nf)(Mg)} \;=\; \overline{MNfg} \;=\; \overline{0}$$

also muss bereits $\overline{Nf} = \overline{0}$ oder $\overline{Mg} = \overline{0}$ gelten. Ohne Einschränkung gelte $\overline{Nf} = \overline{0}$, dann werden alle A_i von p geteilt. Da f normiert ist, wird also insbesondere $A_n = N \cdot a_n = N$ von p geteilt. das heißt es gibt ein $N' \in \mathbb{N}$ mit $N = p \cdot N'$ und $N' < N$. Weiter erfüllt N' die Eigenschaft $N'f \in \mathbb{Z}[X]$. Da N aber als minimal mit dieser Eigenschaft gewählt wurde, muss es ein A_j geben, dass nicht von p geteilt wird. Dies ist offensichtlich Widersprüchlich. ◇

Aus dieser Behauptung folgt die Aussage des Lemmas mit einer einfachen Induktion. □

Satz 7.12 *Ist $\alpha \in \mathcal{O}$ eine ganz-algebraische Zahl, dann hat das Minimalpolynom f_α ganzzahlige Koeffizienten, also $f_\alpha \in \mathbb{Z}[X]$.*

Beweis. Per Definition gibt es ein normiertes Polynom $f \in \mathbb{Z}[X]$ mit $f(\alpha) = 0$. Nach Teil Satz 7.10 **(iii)** wird f von f_α geteilt. Nach Teil **(ii)** des selben Satzes ist f_α ein Primpolynom. Also ein Faktor in der Primzerlegung von f. Mit Lemma 7.11 folgt dann die Behauptung. □