Einführung

Notation & Definitionen

- R ist Platzhalter für $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ oder $\mathbb{F}_p$ (die Menge $\{0, 1, \ldots, p-1\}$ mit Addition und Multiplikation modulo die Primzahl p).
- $R[X]$ ist die Menge der Polynome in der Variable X mit Koeffizienten in R. Polynome könenn addiert und multipliziert werden.
- Ein Element $f \in R[X]$ heißt
  - *invertierbar*, wenn es ein $g \in R[X]$ gibt, sodass $fg = 1$
  - *irreduzibel*, wenn $f \neq 0$, f nicht invertierbar ist und f nicht das Produkt zweier nicht invertierbarer Elemente ist.

Achtung! $X + 1$ ist irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$, während hingegen $2X + 2$ in $\mathbb{Q}[X]$ aber nicht in $\mathbb{Z}[X]$ irreduzibel ist. Denn 2 ist in $\mathbb{Q}$ invertierbar, aber nicht in $\mathbb{Z}$.

Satz 1. *$R[X]$ ist* nullteilerfrei*, d.h. wenn $fg = 0$ für $f, g \in R[X]$, dann ist $f = 0$ oder $g = 0$.*

Primfaktoren

Satz 2. *Jedes $f \in R[X] \setminus \{0\}$ ist ein Produkt von irreduziblen Polynomen, und die irreduziblen Faktoren sind eindeutig bestimmt bis auf Multiplikation mit invertierbaren Elementen.*

$R =$	Invertierbare Elemente in $R[X]$	Grad von irreduziblen Elementen in $R[X]$	Beispiel: Faktorisierung von $5X^4 - 10$ in $R[X]$
$\mathbb{Z}$	± 1	≥ 0	$5(X^4 - 2)$
$\mathbb{Q}$	Grad 0 Polys	≥ 1	$(5X^4 - 10)$
$\mathbb{R}$	Grad 0 Polys	1 oder 2	$(5X - 5\sqrt[4]{2})(X + \sqrt[4]{2})(X^2 + \sqrt{2})$
$\mathbb{C}$	Grad 0 Polys	1	$(5X - 5\sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2})$
$\mathbb{F}_2$	Grad 0 Polys	≥ 1	$(X)^4$
$\mathbb{F}_3$	Grad 0 Polys	≥ 1	$(-X^2 - X + 1)(X^2 - X - 1)$
$\mathbb{F}_5$	Grad 0 Polys	≥ 1	$0 \Longrightarrow$ keine Faktorisierung

Korollar 3. *Für $f, g \in R[X]$ (nicht beide 0) ist $ggT(f, g)$ wohldefiniert bis auf Multiplikation mit invertierbaren Elementen. Für $R \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p\}$ ist $ggT(f, g)$ eindeutig bestimmt, wenn wir fordern, dass er monisch ist.*

Komplexe Wurzeln & Minimalpolynom

Satz 4. *Sei $f(X) \in \mathbb{C}[X]$ vom Grad $n \geq 1$. Dann existieren $\alpha_1, \ldots, \alpha_n, c \in \mathbb{C}$, sodass $f(X) = c(X - \alpha_1) \ldots (X - \alpha_n)$.*

Satz 5. *Sei $\alpha \in \mathbb{C}$ sodass $f(\alpha) = 0$ für irgendein $f \in \mathbb{Q}[X] \setminus \{0\}$ gilt. (Solche α heißen* algebraische Zahlen*.) Sei $M_\alpha \in \mathbb{Q}[X]$ das monische Polynom kleinsten Grades, sodass $M_\alpha(\alpha) = 0$. (M_α wird* Minimalpolynom von α *genannt.) Es gilt:*

- *M_α ist eindeutig bestimmt und irreduzibel in $\mathbb{Q}[X]$.*
- *Für jedes $g \in \mathbb{Q}[X]$ mit $g(\alpha) = 0$ gilt $m_\alpha | g$.*

Ist $M_\alpha \in \mathbb{Z}[X]$, wird α eine *ganze* algebraische Zahl genannt.

Geometrie der komplexen Zahlen

Unter $\mathbb{C} \cong \mathbb{R}^2$ entspricht Addition in $\mathbb{C}$ der Vektoraddition in $\mathbb{R}^2$. Bei der Multiplikation in $\mathbb{C}$ multipliert sich der Betrag ($|a \cdot b| = |a| \cdot |b| \ \ \forall a, b \in \mathbb{C}$) und addiert sich der Winkel zur positiven reellen Achse. Die komplexe Zahl mit Betrag $r \geq 0$ und Winkel ϕ zur positiven reellen Achse ist durch $re^{i\phi}$ gegeben, wobei ϕ im Bogenmaß gegeben sein muss ($360° = 2\pi$). Wie auch in $\mathbb{R}^2$ gilt die Dreiecksungleichung $|a + b| \leq |a| + |b|$.

Aufgaben

Mit $*$ sind optional, da sie entweder einen Satz aus der komplexen Analysis benötigen (Satz von Rouché) oder für ihre Lösungen aus Zeitgründen auf die Quellenangaben (s.u.) verwiesen wird.

Aufgabe 1 (Inhalt eines Polynoms)**.** Definiere für jedes $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X] \setminus \{0\}$ den *Inhalt* $c(f)$ *von* f durch $c(f) := \mathrm{ggT}(a_0, a_1, \ldots, a_n)$. Beweise, dass $c(fg) = c(f)c(g)$ für alle $f, g \in \mathbb{Z}[X] \setminus \{0\}$ gilt.

Anmerkung: Polynome mit $c(f) = 1$ werden *primitiv* genannt.

Aufgabe 2 (Lemma von Gauß)**.** Sei $f(X) \in \mathbb{Z}[X] \setminus \{0\}$ mit $\deg(f) \geq 1$. Zeige, dass f dann und nur dann irreduzibel in $\mathbb{Z}[X]$ ist, wenn es irreduzibel in $\mathbb{Q}[X]$ ist und $c(f) = 1$ gilt.

Aufgabe 3. Seien $a_1, \ldots, a_n$ verschiedene ganze Zahlen.

(a) Zeige, dass $f(x) := (x - a_1) \ldots (x - a_n) - 1 \in \mathbb{Z}[x]$ irreduzibel ist.

(b) Nimm außerdem an, dass n ungerade ist. Zeige, dass $f(x) := (x - a_1) \ldots (x - a_n) + 1 \in \mathbb{Z}[x]$ irreduzibel ist.

Aufgabe 4. Für $f(X) = \sum_{k=0}^{n} a_k X^k \in R[X]$ mit $a_n \neq 0$ definiere $\widehat{f}(X) := \sum_{k=0}^{n} a_{n-k} X^k \in R[X]$. Beweise, dass f dann und nur dann irreduzibel in $R[X]$ ist, wenn $\widehat{f}$ irreduzibel in $R[X]$ ist.

Aufgabe 5 (Irreduzibilitätskriterium von Eisenstein)**.** Sei $f = \sum_{i=0}^{m} a_i x^i \in \mathbb{Z}[x]$ ein primitives Polynom, sodass $p \nmid a_n$, $p \mid a_0, \ldots, a_{n-1}$, $p^2 \nmid a_0$. Zeige, dass f irreduzibel ist.

Verallgemeinerung: Wenn $p | a_0, a_1, \ldots, a_{k-1}$, $p \nmid a_k$ und $p^2 \nmid a_0$, dann hat f einen irreduziblen Faktor dessen Grad mindestens k ist.

Aufgabe 6. Sei $f(X) = (2^5 - 1)X^4 + (2^{10} - 1)X^3 + (2^{15} - 1)X^2 + (2^{18} - 1)$. Zeige, dass f irreduzibel in $\mathbb{Z}[X]$ ist.

Aufgabe 7. Sei p eine Primzahl und definiere $\Phi_p(X) = X^{p-1} + \cdots + X + 1$. Zeige, dass $\Phi_p(X)$ irreduzibel in $\mathbb{Z}[X]$ ist.

Aufgabe 8. Was passiert, wenn wir $\Phi_p(X)$ stattdessen modulo p betrachten, also als Element von $\mathbb{F}_p[X]$? Faktorisiere $\Phi_p(X)$ in $\mathbb{F}_p[X]$.

Hinweis: Tatsächlich ist das n-te Kreisteilungspolynom $\Phi_n(X) \in \mathbb{Z}[X]$ für alle n irreduzibel. Achtung: Die Definition von $\Phi_n(X)$ folgt nicht der einfachen Formel von $\Phi_p(X)$.

Aufgabe 9. Faktorisiere $X^{p-2} + X^{p-3} + \cdots + X + 1$ in $\mathbb{F}_p[X]$, wobei p eine Primzahl ist. Leite daraus den Satz von Wilson und andere Identitäten modulo p ab.

Aufgabe 10. Sei $f \in \mathbb{Z}[X]$ ein monisches Polynom, dessen komplexe Wurzeln alle auf oder innerhalb des Einheitskreises liegen. Zeige, dass jede komplexe Wurzel von f entweder eine Einheitswurzel oder 0 ist, also $f | x^k (x^m - 1)^k$ für irgendwelche $m, k \in \mathbb{N}_{>0}$.

Aufgabe 11. Finde ein irreduzibles Polynom in $\mathbb{Z}[X]$, das reduzibel modulo jede Primzahl p ist.

Aufgabe 12. Sei $n \geq 2$ eine ganze Zahl. Zeige, dass $X^n + X + 3$ irreduzibel in $\mathbb{Z}[X]$ ist.

Aufgabe 13. Sei $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ mit $|a_0|$ prim und $|a_0| > |a_1| + |a_2| + \cdots + |a_n|$. Dann ist f irreduzibel in $\mathbb{Z}[X]$.

$*$ **Aufgabe 14.** Sei $f(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$ mit $|a_k| > |a_0| + |a_1| + \cdots + |a_{k-1}| + |a_{k+1}| + \cdots + |a_n|$. Dann liegen genau k komplexe Wurzeln von f strikt im Inneren des Einheitskreises, und die restlichen $n-k$ Wurzeln liegen strikt außerhalb des Einheitskreises.

Aufgabe 15 (Irreduzibilitätskriterium von Perron)**.** Sei $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ mit $a_0 \neq 0$ und $|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|$. Dann ist f irreduzibel.

Aufgabe 16. Sei $f(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{R}[X]$ ein Polynom mit $0 < a_0 \leq a_1 \leq \cdots \leq a_n$, und sei $z \in \mathbb{C}$ mit $f(z) = 0$. Dann gilt $|z| \leq 1$.

Aufgabe 17. Sei $f(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{R}[X]$ ein Polynom mit positiven Koeffizienten, und sei $z \in \mathbb{C}$ mit $f(z) = 0$. Dann gilt

$$\min_{1 \leq k \leq n} \frac{a_{k-1}}{a_k} \leq |z| \leq \max_{1 \leq k \leq n} \frac{a_{k-1}}{a_k}.$$

Aufgabe 18. Sei p eine Primzahl. Zeige, dass das Polynom $f(X) = X^{p-1} + 2X^{p-2} + \cdots + (p-1)X + p$ irreduzibel in $\mathbb{Z}[X]$ ist.

Aufgabe 19 (Brasilien 2006)**.** Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom mit zwei verschiedenen komplexen Wurzeln, deren Produkt eins ist. Beweise, dass der Grad von f gerade ist.

Aufgabe 20. Seien m, n, a positive ganze Zahlen und $p < a - 1$ eine Primzahl. Beweise, dass $f(X) := X^m (X-a)^n + p \in \mathbb{Z}[X]$ irreduzibel ist.

Aufgabe 21 (Iran TST 2007)**.** Gibt es eine Folge $a_0, a_1, a_2, \ldots$ in $\mathbb{N}$ mit $\mathrm{ggT}(a_i, a_j) = 1$ für alle $i \neq j$, sodass für alle $n \in \mathbb{N}$ das Polynom $\sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ irreduzibel ist?

Aufgabe 22 (MOP 2007)**.** Sei $p(X) \in \mathbb{Z}[X]$. Gibt es eine positive ganze Zahl k, sodass $p(X) - k$ irreduzibel in $\mathbb{Z}[X]$ ist?

Aufgabe 23. Emmy und Sophie spielen ein Spiel. Emmy denkt sich ein Polynom $P(X)$ mit nichtnegativen ganzzahligen Koeffizienten aus. Sophie darf sich eine Zahl $a \in \mathbb{Z}$ aussuchen und von Emmy den Wert $P(a)$ erfahren. Dann darf Sophie sich eine zweite Zahl $b \in \mathbb{Z}$ aussuchen und von Emmy den Wert $P(b)$ erfahren. Anschließend muss Sophie $P(X)$ erraten. Hat sie eine Gewinnstrategie?

$*$ **Aufgabe 24** (Irreduzibilitätskriterium von Cohn)**.** Sei p eine Primzahl und $b \geq 2$ eine natürliche Zahl. Sei $\overline{p_n p_{n-1} \ldots p_1 p_0}$ die Darstellung der Zahl p zur Basis b mit $0 \leq p_i < b$ für jedes i und $p_n \neq 0$. Dann ist das Polynom

$$f(x) := p_n x^n + \cdots + p_1 x + p_0 \in \mathbb{Z}[x]$$

irreduzibel.

$*$ **Aufgabe 25** (Irreduzibilitätskriterium von Dumas)**.** Sei $f(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ und p eine Primzahl. Wenn

(i) $\frac{\nu_p(a_i)}{i} > \frac{\nu_p(a_n)}{n}$ für $i \in \{1, 2, \ldots, n-1\}$,

(ii) $\nu_p(a_0) = 0$ und

(iii) $\mathrm{ggT}(\nu_p(a_n), n) = 1$,

dann ist f irreduzibel in $\mathbb{Q}[X]$. Hierbei ist $\nu_p(a_i)$ die größte ganze Zahl k, sodass $p^k | a_i$. Per Konvention gilt $\nu_p(0) = \infty$.

Anmerkungen: Dieses Kriterium lässt zahlreiche Verallgemeinerungen zu, indem die Eigenschaften des Newton-Polygons von f für verschiedene Primzahlen p verglichen werden (siehe [1]). Das *Newton-Polygon* von f zur Primzahl p erhält man, indem man die Punkte $(i, \nu_p(a_i)) \in \mathbb{R}^2$ für $i = 0, 1, \ldots, n$ aufzeichnet und die untere konvexe Hülle dieser Punktmenge nimmt (siehe [7]). Es beschreibt die p-adischen Bewertungen der Wurzeln von f in den verfollständigten p-adischen Zahlen $\mathbb{C}_p$.

Eine elementare Erklärung, warum das Newton-Polygon etwas mit Irreduzibilität zu tun haben sollte, findet sich in [2].

Quellen und weiterführende Literatur

[1] Bonciocat, Nicolae Ciprian. "Schönemann–Eisenstein–Dumas-Type Irreducibility Conditions That Use Arbitrarily Many Prime Numbers." Communications in Algebra 43, no. 8 (August 3, 2015): 3102–22. https://doi.org/10.1080/00927872.2014.910800.

Aufgabe 5,24

[2] Captain Lama (https://math.stackexchange.com/users/318467/captain-lama), Antwort auf StackExchange zu "Explaining Newton Polygon for proving irreducibility of polynomial in $\mathbb{Z}[x]$ in elementary way". https://math.stackexchange.com/q/1678839, zuletzt aufgerufen am 26. Oktober 2023.

Aufgabe 5,25

[3] Chua, D., Part IB Groups, Rings, and Modules, lectured by O. Randal-Williams. *University of Cambridge*, Lent 2016. https://dec41.user.srcf.net/h/IB_L/groups_rings_and_modules, zuletzt aufgerufen am 26. Oktober 2023.

Aufgabe 1,2,5,7

[4] Gosh, A., "Irreducibility of Integer Polynomials". https://ghoshadi.files.wordpress.com/2020/04/irreducibility-of-integer-polynomials.pdf, zuletzt aufgerufen am 4. Oktober 2023.

Aufgabe 3,4–6,20

[5] Grojnowski, Ian. Part II Galois Theory, Example Sheet 1. *University of Cambridge*, October 2019. URL: https://www.dpmms.cam.ac.uk/study/II/Galois/2019-2020/ex1.pdf, zuletzt aufgerufen am 26. Oktober 2023.

Aufgabe 11

[6] Kronecker, L. "Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten." Journal Für Die Reine Und Angewandte Mathematik (Crelles Journal) 1857, no. 53 (January 1, 1857): 173–75. https://doi.org/10.1515/crll.1857.53.173.

Aufgabe 10

[7] Wikipedia, Newton polygon. https://en.wikipedia.org/wiki/Newton_polygon, zuletzt aufgerufen am 26.10.2023.

Aufgabe 5,25

[8] Zhao, J. "Integer Polynomials", MOP 2007 Black Group (June 29, 2007). https://yufeizhao.com/olympiad/intpoly.pdf, zuletzt aufgerufen am 4. Oktober 2023.

Aufgabe 5,7,13–24