# Nachtrag zu Faktorgruppen

## H21T1A4 (a) (teilweise)

Zeigen Sie, dass $\mathbb{Q}/\mathbb{Z}$ eine unendliche Gruppe ist.

Beh.: $A = \{\frac{1}{n} + \mathbb{Z} \mid n \in \mathbb{N}\}$ ist eine unendl. Teilmenge von $\mathbb{Q}/\mathbb{Z}$ (Daraus folgt $|\mathbb{Q}/\mathbb{Z}| = \infty$.)

Es genügt zzg.: $\forall m, n \in \mathbb{N} \cdot m < n \Rightarrow \frac{1}{m} + \mathbb{Z} \neq \frac{1}{n} + \mathbb{Z}$

Seien also $m, n \in \mathbb{N}$ mit $m < n$ vorreg. Ang. $\frac{1}{m} + \mathbb{Z} = \frac{1}{n} + \mathbb{Z}$.

$\Rightarrow \frac{1}{m} - \frac{1}{n} = a$ fixo em $a \in \mathbb{Z}$

$\Rightarrow n - m = a\,m\,n \Rightarrow n \mid (n-m) \Rightarrow$

$n \mid m \lightning$ da $m, n \in \mathbb{N}$, $m < n$ $\square$

# Überblick Irreduzibilitätskriterien

(1) Irreduzibilität in $\mathbb{Z}[x]$ vs. Irreduzibilität in $\mathbb{Q}(x)$

- „$f \in \mathbb{Z}[x]$ irred. in $\mathbb{Z}[x] \Rightarrow f$ irred. in $\mathbb{Q}[x]$" ist immer erfüllt
- Die Umkehrung der Implikation gilt nur, wenn $f \in \mathbb{Z}[x]$ ein <u>primitives</u> Polynom ist, d.h. wenn die Koeff. von $f$ keinen gem. Primteiler haben.

(Bsp. $f = 2x+4$ ist irred. in $\mathbb{Q}[x]$, aber nicht in $\mathbb{Z}[x]$

da $f = 2 \cdot (x+2)$ eine Zerlegung in Nichteinheiten ist)

(2) Irreduzibilität anhand des Polynomgrads

Sei $K$ ein Körper und $f \in K[x] \setminus K$.

- Ist $\operatorname{grad}(f) = 1$, dann ist $f$ irred in $K[x]$.
- Ist $\operatorname{grad}(f) \in \{2,3\}$ und hat $f$ in $K$ keine Nullstelle, dann ist $f$ irred in $K[x]$.
- Ist $\operatorname{grad}(f) \in \{4,5\}$, hat $f$ in $K$ keine Nullstelle und wird $f$ nicht durch ein irred. Pol. vom Grad 2 geteilt, dann ist $f$ irreduzibel in $K[x]$.

## (3) Untersuchung eines Polynoms $f \in \mathbb{Z}[x]$ auf rationale Nullstellen

Sei $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ mit $n \in \mathbb{N}$, $a_n \neq 0$. Ist $x = \frac{p}{q} \in \mathbb{Q}$ eine Nullstelle von $f$ mit $p, q \in \mathbb{Z}$, $q \neq 0$, $ggT(p,q) = 1$, dann folgt $p \mid a_0$ und $q \mid a_n$.

(Spezialfall: Ist $f$ normiert ($a_n = 1$), dann ist jede rationale Nullstelle ganzzahlig und ein Teiler von $a_0$.)

(4) Reduktionskriterium:

Sei $f = x^n + a_{n-1}x + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$, $p$ eine Primzahl und $\bar{f}$ das Bild von $f$ in $\mathbb{F}_p[x]$. Ist $\bar{f}$ irred. in $\mathbb{F}_p[x]$, dann ist $f$ irreduzibel in $\mathbb{Z}[x]$.

(Achtung: Aus der Reduzibilität von $\bar{f}$ folgt nicht, dass $f$ reduzibel ist. Zum Beispiel ist $\bar{f} = x^2 + \bar{1} \in \mathbb{F}_2[x]$ reduzibel wg. $\bar{f} = (x+\bar{1})^2$, aber $f = x^2 + 1$ ist in $\mathbb{Z}[x]$ irreduzibel.)

(5) Eisenstein-Kriterium: Sei $f = a_n x^n + \dots + a_1 x \in \mathbb{Z}[x]$ primitiv und $p$ eine Primzahl, so dass $p \nmid a_n$, $p \mid a_k$ für $0 \le k < n$, $p^2 \nmid a_0$, dann

ist $f$ in $\mathbb{Z}[x]$ irreduzibel (und damit auch in $\mathbb{Q}[x]$, nach (1)).

F20T3AS (Übung: F13T1A2)

Sei $f_1 = x^5 + 10x + 5 \in \mathbb{Z}[x]$, und es sei die Folge $(f_n)_{n \in \mathbb{N}}$ in $\mathbb{Z}[x]$ rekursiv definiert durch $f_n(x) = f_1(f_{n-1}(x))$ $\forall\, n \geq 2$. Zeigen Sie, dass $f_n$ für jedes $n \in \mathbb{N}$ irreduzibel ist. Gehen Sie dabei folgendermaßen vor:

(a) Zeigen Sie, dass das Bild von $f_n$ in $\mathbb{Z}/5\mathbb{Z}[x]$ mit $x^{5^n}$ übereinstimmt, für jedes $n \in \mathbb{N}$.

(b) Zeigen Sie, dass das Bild von $f_n(0)$ in $\mathbb{Z}/25\mathbb{Z}$ für jedes $n \in \mathbb{N}$ ungleich $\bar{0}$ ist.

$f \in \mathbb{Z}[x]$

$n \in \mathbb{N}$

llstelle

$(p,q) = 1$,

st $(a_n = 1)$,

lle ganz-

)

Zeige zunächst, dass aus (a), (b) für jedes $n \in \mathbb{N}$ die Irred. von $f_n$ in $\mathbb{Z}[x]$ folgt.

Sei $n \in \mathbb{N}$. Dann hat $f$ eine Darstellung

$f_n = \sum_{k=0}^{r} a_k x^k$ mit $r \in \mathbb{N}$ und $a_0, \dots, a_r \in \mathbb{Z}$,

$a_0 \neq 0$. Beh.: $r = 5^n$

Es genügt durch vollst. Ind $z$ zu zeigen, dass

$\operatorname{grad} f_m = 5^m \quad \forall m \in \mathbb{N}$ gilt. Für $m = 1$

ist das offensichtlich, und aus $\operatorname{grad}(f_m)$

$= 5^m$ folgt $\operatorname{grad}(f_m^5) = 5 \cdot \operatorname{grad}(f_m)$

$= 5 \cdot 5^m = 5^{m+1}$ und somit $\operatorname{grad}(f_{m+1}) =$

$\operatorname{grad}(f_m^5 + f_m + 5) = \operatorname{grad}(f_m^5) = 5^{m+1}$

Zeige nun, dass $f_n$ die Vor. des Eisensteinkrit. erfüllt.

$f_n$ normiert $\Rightarrow$ $f_n$ ist primitiv

Sei $\bar{f}_m$ das Bild von $f_m$ in $\mathbb{Z}/5\mathbb{Z}[x]$. Teil (a) $\Rightarrow$

$x^{5^m} = \bar{a}_r x^{5^m} + \dots + \bar{a}_1 x + \bar{a}_0$ in $\mathbb{Z}/5\mathbb{Z}$

$\Rightarrow \bar{a}_r = \bar{1}$, $\bar{a}_k = \bar{0}$ für $0 \leq k < r$

$\Rightarrow 5 \mid a_r$, $5 \mid a_k$ für $0 \leq k < r$

Teil (b) $\Rightarrow \bar{a}_0 = \overline{f(0)} \neq \bar{0}$ in $\mathbb{Z}/25\mathbb{Z}$

$\Rightarrow 5^2 \nmid a_0$ Also sind die Vor. des Eisenstein-Krit. erfüllt und $f_n$ somit irred. in $\mathbb{Z}[x]$.

bei (b) $\Rightarrow \bar{a}_0 = f(0) \neq \bar{0}$ in $\mathbb{Z}/25\mathbb{Z}$

$\Rightarrow 5^2 \nmid a_0$ Also sind die Vor. des Eisenstein-Kri.

zu (a) durch vollst. Ind. über $n \in \mathbb{N}$

Ind.-Anf. Das Bild von $f_1$ in $\mathbb{Z}/5\mathbb{Z}$ ist

$$x^5 + \bar{10}x + \bar{5} = x^5 = x^{5^1}$$

Ind.-Schritt $n \mapsto n+1$ Ind.-V. $\Rightarrow \bar{f}_{f_n} = x^{5^n}$ in $\mathbb{Z}/5\mathbb{Z}[x]$

$$\Rightarrow \bar{f}_{f_{n+1}} = \bar{f}_1(\bar{f}_{f_n}) = \bar{f}_{f_n}^5 + \bar{10}\,\bar{f}_{f_n} + \bar{5} =$$

$$\bar{f}_{f_n}^5 = (x^{5^n})^5 = x^{5^{n+1}}$$

zu (b) durch vollst. Ind. über $n$

Ind.-Anf.: $f_1(0) = 5$ ist nicht durch 25 teilbar

Ind.-Schritt: $n \mapsto n+1$ Vor.: $f_n(0)$ nicht teilbar durch 25

Da das Bild von $f_n$ in $\mathbb{Z}/5\mathbb{Z}$ gleich $\pm 5^n$ ist,

gilt $\overline{f_n(0)} = \bar{0}^{5^n} = \bar{0}$ in $\mathbb{Z}/5\mathbb{Z} \Rightarrow$

$f_n(0)$ ist teilbar durch 5

$f_{n+1}(0) = f_1(f_n(0)) = f_n(0)^5 + 10 f_n(0) + 5$

Aus $5 \mid f_n(0)$ folgt $25 \mid f_n(0)^5$ und $25 \mid 10 f_n(0)$

Wäre $f_{n+1}(0)$ durch 25 teilbar, dann würde

$25 \mid 5$ folgen. $\lightning$. also: $25 \nmid f_{n+1}(0)$ $\square$

# F13T3 A4

(a) Bestimmen Sie alle normierten, irred. Polynome vom Grad $\leq 2$ in $\mathbb{F}_3[x]$.

- Das einzige normierte Pol. vom Grad 0 ist $\overline{1}$, und dies ist eine Einheit, kein irred. Element.
- Normierte Pol. vom Grad 1 sind alle irreduzibel. Dies sind $x$, $x+\overline{1}$ und $x+\overline{2}$.
- Ein normiertes Polynom vom Grad 2 ist genau dann irred., wenn es in $\mathbb{F}_3$ keine Nullstelle hat. Die normierten Pol. vom Grad 2 mit Nullstelle sind die mit konstantem Term 0, und

laut Vorlesung in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$ irreduzibel

$(x+\bar{1})^2 = x^2+\bar{2}x+\bar{1}$, $(x+\bar{2})^2 = x^2+\bar{4}x+\bar{4}$

$= x^2+x+\bar{1}$ und $(x+\bar{1})(x+\bar{2}) = x^2+\bar{2}$

Als irreduzible Polynome bleiben somit übrig: $x^2+\bar{1}$, $x^2+x+\bar{2}$, $x^2+\bar{2}x+\bar{2}$

Insg. gibt es also 6 irred. normierte Polynome vom Grad $\leq 2$ in $\mathbb{F}_3[x]$.

(b) Zeigen Sie, dass $f = x^4-9x^2-2x+2$ in $\mathbb{Z}[x]$ irreduzibel ist.

Auf Grund des Reduktionskriteriums genügt es zu überprüfen, dass $f$ normiert (offenbar erfüllt) und dass das Bild $\bar{f}$ von $f$ in $\mathbb{F}_3[x]$ irreduzibel ist.

Es ist $\bar{f} = x^4 + \bar{x} + \bar{2}$ Wegen grad $(\bar{f}) = 4$ genügt es zu überprüfen, dass $\bar{f}$ in $\mathbb{F}_3$ keine Nullstelle hat und kein Produkt zweier irred. Polynome vom Grad 2 ist.

$\bar{f}(\bar{0}) = \bar{2} \neq \bar{0}$, $\bar{f}(\bar{1}) = \bar{4} = \bar{1} \neq \bar{0}$, $\bar{f}(\bar{2}) = \overline{20}$
$= \bar{2} \neq \bar{0}$

Da der konstante Term von $\bar{f}$ gleich $\bar{2}$ ist, kann $\bar{f}$ kein Produkt von $x^2 + x + \bar{2}$ und $x^2 + \bar{2}x + \bar{2}$ sein, und auch kein Quadrat eines dieser Polynome. Einzige Möglichkeit also: $\bar{f} = (x^2 + \bar{1})(x^2 + x + \bar{2})$ oder $\bar{f} = (x^2 + \bar{1})(x^2 + 2x + \bar{2})$ Aber Nachrechnen (ausführen!) ergibt, dass beide Gleichungen falsch sind). □

Übung: Zeigen Sie, dass $x^4 - 2x^3 + 4x^2 - 7x + 5$ in $\mathbb{Z}[x]$ irreduzibel ist.

Ergänzungen:

- Alle Kreisteilungspolynome $\Phi_n$ sind laut Vorlesung in $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$ irreduzibel
- Ist $K$ ein Körper, $f \in K[x]$ und $a \in K$, dann gilt die Äquivalenz

  $f$ irred. in $K[x] \iff f(x-a)$ irred in $K[x]$

(Auf diese Weise kann z.B. die Irreduzibilität von $\Phi_p = x^{p-1} + x^{p-2} + \dots + x + 1$ für jede Primzahl $p$ auf das Eisenstein-Kriterium zurückgeführt

werden.)

- Ist $K$ ein Körper, $L \supseteq K$ ein Erweiterungskörper, $f \in K[x] \setminus \{0\}$ und $\alpha \in L$ mit $f(\alpha) = 0$ und $[K(\alpha) : K] = \operatorname{grad}(f)$, dann ist $f$ irred. in $K[x]$.

(Bsp.: Ist $f \in \mathbb{Q}[x]$ vom Grad 2 und $1+\sqrt{2}$ eine Nullstelle von $f$ (z.B. $f = x^2 - 2x - 1$) dann ist $f$ irreduzibel, wegen $[\mathbb{Q}(1+\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 = \operatorname{grad}(f)$.)