

Aufgabe (zur Jahreszahl 2026)

$$\text{Es ist } 2026 = 1 + 45^2 \quad (*)$$

(a) Zeigen Sie, dass 2 und 1013 in $R = \mathbb{Z}[\sqrt{2026}]$ irreduzibel, aber nicht prim sind. Schließen Sie daraus, dass R kein faktorieller Ring ist.

(b) Im Ring $\mathbb{Z}[i]$ der Gauß'schen Zahlen gilt $2026 = (1+i)(1-i)1013$. Verwenden Sie dies zusammen mit (*), um

14

die Zahl 1013 als Summe von zwei Quadraten darzustellen.

Endliche Körper

Hauptsatz

(1) Ist K ein endlicher Körper, dann gibt es eine Primzahl p und ein $n \in \mathbb{N}$ mit $|K| = p^n$.

Dabei ist $p = \text{char}(K)$ (und zugleich die Elementarzahl des Primkörpers P) und $n = [K : P]$.

(2) Umgekehrt existiert für jede Primzahlpotenz $q > 1$ ein Körper mit q Elementen, und dieser Körper ist bis auf Isomorphie eindeutig bestimmt.

(3) Sei K ein Körper mit p^n Elementen (p Primzahl, $n \in \mathbb{N}$). Sei P der Primkörper von K . Dann ist K der Zerfällungskörper des Polynoms $f_n = x^{p^n} - x \in P[x]$, und die Elemente von K sind genau die Nullstellen von f_n .

(4) Ist K ein Körper mit q Elementen ($q > 1$ Primzahlpotenz), dann ist $K^\times$ eine zyklische Gruppe der Ordnung $q-1$.

(3) Sei K ein Körper mit p^n Elementen (p Primzahl, $n \in \mathbb{N}$)
 Sei P der Primkörper von K . Dann ist K der Zerfällungskörper des Polynoms $f_n = x^{p^n} - x \in P[x]$ und die Elemente von

(5) Sei p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Sei $\mathbb{F}_p^{\text{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_p$.

Dann gibt es für jedes $n \in \mathbb{N}$ genau einen Zwischenkörper mit p^n Elementen, der üblicherweise mit $\mathbb{F}_{p^n}$ bezeichnet wird. Dabei gilt

$$(i) [\mathbb{F}_{p^n} : \mathbb{F}_p] = n \quad \forall n \in \mathbb{N}$$

$$(ii) \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n \quad (\forall m, n \in \mathbb{N})$$

$$(iii) \mathbb{F}_p^{\text{alg}} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$$

Hinweise : • Für $n \geq 2$ sind $\mathbb{F}_{p^n}$ und $\mathbb{Z}/p^n\mathbb{Z}$ nicht isomorph (erst recht nicht gleich).

• Aus $p^m \mid p^n$ folgt im Allg. nicht $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, z.B. $\mathbb{F}_4 \not\subseteq \mathbb{F}_8$.

- Sei p eine Primzahl und $n \in \mathbb{N}$.

Dann gibt es ein irreduzibles Polynom $f \in \mathbb{F}_p[x]$ vom Grad n und eine Nullstelle $\alpha \in \mathbb{F}_{p^n}$ von f , so dass die Elemente von $\mathbb{F}_{p^n}$ durch $\{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_0, \dots, a_{n-1} \in \mathbb{F}_p\}$ geg. sind, d.h.

$\{1, \alpha, \dots, \alpha^{n-1}\}$ bilden eine Basis von $\mathbb{F}_{p^n}$ als $\mathbb{F}_p$ -Vektorraum.

Bsp. Es gibt eine Nullstelle $\alpha \in \mathbb{F}_4$ von $f = x^2 + x + 1 \in \mathbb{F}_2[x]$ mit $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$. $f(\alpha) = 0 \Rightarrow \alpha^2 + \alpha + 1 = 0 \Rightarrow \alpha^2 = -1 - \alpha = 1 + \alpha$. Dies kann zur

$$p^2 \equiv$$

Also

wegen

$$p \equiv 1$$

$$p^2 \equiv 3$$

F23T2

von $\mathbb{F}_6$

$$\alpha \in \mathbb{F}_6 +$$

Allgemein

$\Rightarrow$ Primzahl

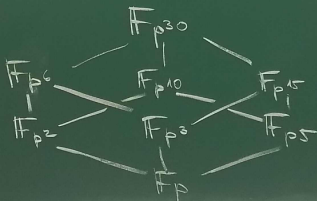
außerdem

Multiplikation von Elementen genutzt werden.

Zum Beispiel ist $\alpha \cdot (\bar{1} + \alpha) = \alpha + \alpha^2 = \alpha + (\bar{1} + \alpha) = \bar{1} + \bar{2}\alpha = \bar{1}. (\Rightarrow \bar{1} + \alpha = \alpha^{-1})$

Übung. Sei $\mathbb{F}_8$ ein Erweiterungskörper von $\mathbb{F}_2$ mit $|\mathbb{F}_8| = 8$ und α eine Nullstelle von $f = x^3 + x + \bar{1} \in \mathbb{F}_2[x]$. Geben Sie alle Elemente von $\mathbb{F}_8$ an sowie die Verknüpfungstabellen für Addition und Multiplikation.

Beispiel zu (ii): Teilkörper von $\mathbb{F}_{p^{30}}$ (p Primzahl)



F24TZA1 (G)

Sei p eine Primzahl mit $p > 3$. Zeigen Sie, dass $\mathbb{F}_{p^2}^\times$ ein Element der Ordnung 12 enthält.

bekannt: $\mathbb{F}_{p^2}^\times$ ist eine zyklische Gruppe der Ordnung $p^2 - 1$. Daraus folgt, dass es für jeden Teiler $d \in \mathbb{N}$ von $p^2 - 1$ in $\mathbb{F}_{p^2}^\times$ ein Element der Ordnung d gibt. Es genügt also zu zeigen, dass 12 ein Teiler von $p^2 - 1$ ist. Es ist $12 = 3 \cdot 4$, und $\text{ggT}(3, 4) = 1 \Rightarrow$ Es reicht zu zeigen, dass $3 \mid (p^2 - 1)$ und $4 \mid (p^2 - 1)$, was zu $p^2 \equiv 1 \pmod{3}$ und $p^2 \equiv 1 \pmod{4}$ äquivalent ist.

$p > 3 \Rightarrow 3 \nmid p \Rightarrow p \not\equiv 0 \pmod{3} \Rightarrow$

$$\Rightarrow p \equiv 1 \pmod{3} \text{ oder } p \equiv 2 \pmod{3} \Rightarrow$$

$$p^2 \equiv 1^2 \equiv 1 \pmod{3} \text{ oder } p^2 \equiv 2^2 \equiv 4 \equiv 1 \pmod{3}$$

Also gilt $p^2 \equiv 1 \pmod{3}$ in jedem Fall.

Wegen $p > 2$ ist p eine ungerade Primzahl. $\Rightarrow$

$$p \equiv 1 \pmod{4} \text{ oder } p \equiv 3 \pmod{4} \Rightarrow p^2 \equiv 1^2 \equiv 1 \pmod{4} \text{ oder}$$

$$p^2 \equiv 3^2 \equiv 9 \equiv 1 \pmod{4} \Rightarrow p^2 \equiv 1 \pmod{4} \quad \square$$

F23T2A5 (V) Sei P der Primkörper

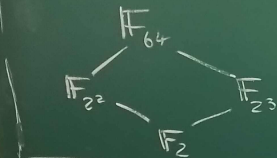
von $\mathbb{F}_{64}$. Bestimmen Sie die Anzahl der Elemente
 $\alpha \in \mathbb{F}_{64}$ mit $\mathbb{F}_{64} = P(\alpha)$.

Allgemein ist $\mathbb{F}_p$ der Primkörper von $\mathbb{F}_{p^n}$ (falls
 n Primzahl, $n \in \mathbb{N}$) Also ist $P = \mathbb{F}_2$.

außerdem: $64 = 2^6 \Rightarrow$ Für jeden Teiler d von 6 gibt

gibt es genau einen Teilkörper von $\mathbb{F}_{64}$ mit 2^d Elementen, nämlich $\mathbb{F}_{2^d}$, und keine weiteren Teilkörper.

Diagramm der Teilkörper:



Beh.: Für alle $x \in \mathbb{F}_{64}$ gilt die Äquivalenz

$$\mathbb{F}_2(x) \neq \mathbb{F}_{64} \iff x \in \mathbb{F}_4 \cup \mathbb{F}_8$$

" $\Rightarrow$ " Wegen $\mathbb{F}_2(x) \neq \mathbb{F}_{64}$

muss $\mathbb{F}_2(x)$ mit einem der Körper $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$ übereinstimmen. In den ersten beiden Fällen gilt $x \in \mathbb{F}_4$, im dritten Fall in $\mathbb{F}_8$, in jedem Fall also in $\mathbb{F}_4 \cup \mathbb{F}_8$.

" $\Leftarrow$ " Setze $\alpha \in \mathbb{F}_4 \cup \mathbb{F}_8$ voraus.

1. Fall: $\alpha \in \mathbb{F}_4 \Rightarrow \mathbb{F}_2(\alpha) \subseteq \mathbb{F}_4 \subsetneq \mathbb{F}_{64} \Rightarrow \mathbb{F}_2(\alpha) \subsetneq \mathbb{F}_{64}$

2. Fall: $\alpha \in \mathbb{F}_8 \Rightarrow \mathbb{F}_2(\alpha) \subseteq \mathbb{F}_8 \subsetneq \mathbb{F}_{64} \Rightarrow \mathbb{F}_2(\alpha) \subsetneq \mathbb{F}_{64}$

($\Rightarrow$ Beh.) Aus der Behauptung folgt die Äquivalenz $\mathbb{F}_2(\alpha) = \mathbb{F}_{64} \Leftrightarrow \alpha \in \mathbb{F}_{64} \setminus (\mathbb{F}_4 \cup \mathbb{F}_8)$. Also

ist $|\mathbb{F}_{64} \setminus (\mathbb{F}_4 \cup \mathbb{F}_8)|$ die gesuchte Elementenzahl. Es gilt $\mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_2$, denn $\mathbb{F}_4 \cap \mathbb{F}_8$

ist gemeinsamer Teilkörper von $\mathbb{F}_4, \mathbb{F}_8$, und $\mathbb{F}_2$

ist der einzige gemeinsame Teilkörper von $\mathbb{F}_4$

und $\mathbb{F}_8$ (denn: $\mathbb{F}_2 = \mathbb{F}_{2^1}, \mathbb{F}_4 = \mathbb{F}_{2^2}, \mathbb{F}_8 = \mathbb{F}_{2^3}$, und 1

ist der einzige gem. Teiler von 2 und 3)

D
nie
fol
=
Ein
keine
 $x^2 + 2$
die li

$$\begin{aligned}
 &\Rightarrow |\mathbb{F}_4 \cup \mathbb{F}_8| = |\mathbb{F}_4| + |\mathbb{F}_8| - |\mathbb{F}_4 \cap \mathbb{F}_8| \\
 &= 4 + 8 - |\mathbb{F}_2| = 12 - 2 = 10 \Rightarrow |\mathbb{F}_{64} \setminus (\mathbb{F}_4 \cup \mathbb{F}_8)| \\
 &= |\mathbb{F}_{64}| - |\mathbb{F}_4 \cup \mathbb{F}_8| = 64 - 10 = 54
 \end{aligned}$$

$\Rightarrow$ gibt also 54 Elemente $\alpha \in \mathbb{F}_{64}$ mit $\mathbb{F}_2(\alpha) = \mathbb{F}_{64}$.

- Übung:
- Bestimmen Sie die Anzahl der Elemente α in $\mathbb{F}_{p^{30}}$ mit $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^{30}}$, für jede Primzahl p .
 - Bestimmen Sie die Anzahl der Elemente $\alpha \in \mathbb{F}_{64}$ mit der Eigenschaft $\mathbb{F}_4(\alpha) = \mathbb{F}_{64}$.

H2ST1AS

irreduziblen

(a) Bestimmen Sie alle normierten Polynome vom Grad 2 im Polynomring $\mathbb{F}_3[x]$.

Der konstante Term eines irred. Polynoms vom Grad 2 kann nicht null sein (weil sonst x ein Teiler wäre). Die gesuchte Polynommenge ist also enthalten in $\{x^2+ax+b \mid a \in \{0,1,2\}, b \in \{1,2\}\}$
 $= \{x^2+1, x^2+2, x^2+x+1, x^2+x+2, x^2+2x+1, x^2+2x+2\}$

Ein Polynom vom Grad 2 ist genau dann irreduzibel, wenn es (in $\mathbb{F}_3$) keine Nullstelle hat. x^2+2, x^2+x+1 haben 1 als Nullstelle, $x^2+2x+1 = (x+1)^2$ hat 2 als Nullstelle. Nachrechnen zeigt, dass die übrigen Polynome keine Nullstellen in $\mathbb{F}_3$ haben.

Also ist $\{x^2+1, x^2+x+2, x^2+2x+2\}$ die gesuchte Menge.

(b) Zeigen Sie, dass $K = \mathbb{F}_3[x]/(x^2+1)$ ein Körper ist, und bestimmen Sie die Anzahl der Elemente.

Da $\mathbb{F}_3[x]$ als Polynomring über einem Körper ein Hauptidealring und x^2+1 nach (a) ein irred. Element von $\mathbb{F}_3[x]$ ist, ist (x^2+1) in $\mathbb{F}_3[x]$ ein maximales Ideal, und daraus folgt, dass der Faktorring K ein Körper ist.

Allgemein gilt: Ist k ein Körper und $f \in k[x]$ vom Grad n mit $n \in \mathbb{N}$, dann bilden die Polynome vom Grad $< n$ zusammen mit 0_k ein Repräsentantensystem von $k[x]/(f)$. $\Rightarrow S = \{ax+b \mid a, b \in \mathbb{F}_3\}$

ist
 $|K|$
mit

ist Repr.-system von $\mathbb{F}_3[x]/(x^2+1)$. $\Rightarrow$

$|K| = |S| = 3^2 = 9$. Also ist K ein Körper
mit 9 Elementen.

n
ahl

Körper

ein

1) in

gibt, dass

$\in k[x]$ von

norme von

stanten-

$\forall a, b \in \mathbb{F}_3$