Tutorium #12: Antworten zu (wenigstens einmal gestellten) Fragen

17.02.2015

① Begriffe zu Gruppen

Sei G eine Gruppe.

Def. 1: $g \in G$. $Z_g := \{a \in G \mid ag = ga\}$

„Zentralisator von g" = alle Elemente, die mit g kommutieren

Bsp. 1 (Aufg. 7.2): $G = GL_n(K)$ mit $n=3$. (analog für alle n)

a) $g = \begin{pmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3 \end{pmatrix}$ mit $\lambda_i \neq \lambda_j \ \forall i \neq j$

$$a = (a_{ij})_{i,j=1}^3 \in Z_g \iff ag = ga \iff \underbrace{(a_{ij})_{i,j} \cdot \begin{pmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3 \end{pmatrix}}_{= \begin{pmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3 \end{pmatrix} \cdot (a_{ij})_{i,j}}$$

$$\begin{pmatrix} \lambda_1 a_{11} & \lambda_2 a_{12} & \lambda_3 a_{13} \\ \lambda_1 a_{21} & \lambda_2 a_{22} & \lambda_3 a_{23} \\ \lambda_1 a_{31} & \lambda_2 a_{32} & \lambda_3 a_{33} \end{pmatrix}$$

$$\iff (\lambda_j a_{ij})_{i,j} = (\lambda_i a_{ij})_{i,j}$$

$$\begin{pmatrix} \lambda_1 \cdot a_{1j} \\ \lambda_2 \cdot a_{2j} \\ \lambda_3 \cdot a_{3j} \end{pmatrix}$$

$\lambda_i \neq \lambda_j \ \forall i \neq j \Rightarrow a_{ij} = 0 \ \forall i \neq j$

$$\Rightarrow Z_g = \left\{ \begin{pmatrix} a_{11} & & \\ & a_{22} & \\ & & a_{33} \end{pmatrix} \;\middle|\; \begin{array}{l} a_{ii} \neq 0 \ \forall i \\ a_{ii} = a_{jj} \text{ ist zulässig} \end{array} \right\}$$

= invertierbare Diagonalmatrizen.

b) $g = \begin{pmatrix} \lambda & 1 & \\ & \lambda & 1 \\ & & \lambda \end{pmatrix} = J_3(\lambda) = \lambda \cdot E + \underbrace{\begin{pmatrix} 0 & 1 & \\ & 0 & 1 \\ & & 0 \end{pmatrix}}_{n}$

Bem. 1: $Z_g \subset G$ eine UG $\forall g \in G$.

- $a \in Z_g \iff a(\lambda \cdot E + n) = (\lambda \cdot E + n) \cdot a \iff a \cdot n = n \cdot a$

$$a \cdot n = \begin{pmatrix} 0 & a_{11} & a_{12} \\ 0 & a_{21} & a_{22} \\ 0 & a_{31} & a_{32} \end{pmatrix} = (a_{i,j-1})_{i,j=1}^3 \qquad a_{i0} := 0$$

$$n \cdot a = \begin{pmatrix} a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ 0 & 0 & 0 \end{pmatrix} = (a_{i+1,j})_{i,j=1}^3 \qquad a_{n+1,j} := 0$$

- $a_{i,j-1} = a_{i+1,j}$ falls $j \neq 1$ und $i \neq n$
- $a_{n,j-1} = 0 \quad \forall j \in \{2, \dots, n\}$
- $0 = a_{i+1,1} \ \forall i \in \{1, \dots, n-1\}$

$\Rightarrow \quad Z_g = \{ \begin{pmatrix} a_{11} & a_{21} & a_{31} \\ 0 & a_{11} & a_{21} \\ 0 & 0 & a_{11} \end{pmatrix} \mid \underbrace{a_{11} \neq 0}_{\text{damit } \det A \neq 0} \} =$

Def. 2: $Z(G) = \{ a \in G \mid ag = ga \ \forall g \in G \}$

„Zentrum von G" = alle Elemente, die mit allen Elementen kommutieren

Bem 2: · $Z(G) = \bigcap_{g \in G} Z_g$ · $Z(G) \lhd G$ · G abelsch $\Leftrightarrow Z(G) = G$

Bsp. 2 (siehe Aufg. 35): $Z(GL_3(K)) = \{ \begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \lambda \end{pmatrix} \mid \lambda \neq 0 \}$

„$\supseteq$": ✓

„$\subseteq$": $Z(G) \subseteq \underbrace{Z_{J_3(\lambda)}}_{\text{aus Bsp. 1}} \cap \underbrace{Z_{\mathrm{diag}(\lambda_1, \lambda_2, \lambda_3)}}_{\text{aus Bsp. 1}} = \{ \begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \lambda \end{pmatrix} \mid \lambda \neq 0 \}.$

Def. 3: Sei $H \subset G$ eine Untergruppe.

$N_G(H) := \{ a \in G \mid aH = Ha \}$

„Normalisator von H" = größte UG von G, in der H normal ist.

Bem 3: · $H \lhd G \Leftrightarrow N_G(H) = G$

· $H \lhd N_G(H) \subset G$, $N_G(H)$ eine UG von G

· $H \lhd J \subset G$, J eine UG $\Rightarrow J \subset N_G(H)$

Bem 4: · $Z(G) \lhd N_G(H)$

· $\forall h \in H: \ Z_h \subset N_G(H). \rightsquigarrow \bigcup_{h \in H} Z_h \subset N_G(H)$

Bsp. 3: $H = \{ \begin{pmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3 \end{pmatrix} \mid \lambda_i \neq 0 \} \subset GL_3(K)$

$$N_G(H) = \left\{ (a_{ij}) \mid \begin{array}{c} \text{in jeder Zeile und} \\ \text{jeder Spalte ist} \\ \text{genau ein Eintrag} \neq 0 \end{array} \right\} \neq \bigcup_{h \in H} Z_h.$$

② Begriffe zu Gruppen-Wirkungen

Sei $G \times M \longrightarrow M$ eine Wirkung / Operation

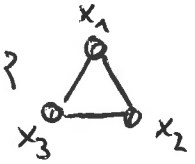
$(g, m) \longmapsto g \cdot m$

Def.: 1) Sei $m \in M$. $G_m := \{ a \in G \mid a \cdot m = m \} \subset G$ Untergruppe
„Stabilisator von m"

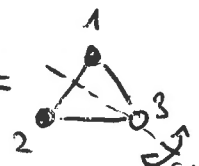
2) Sei $m \in M$. $B_m := \{ a \cdot m \mid a \in G \} \subset M$
„Bahn von m"

3) Sei $g \in G$. $F_g := \{ x \in M \mid gx = x \} \subset M$
„Fixpunktmenge von g"

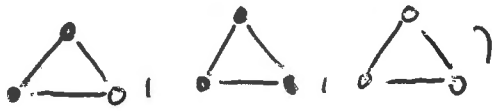
Bsp. 1:

$G = \Sigma_3$ $\quad M = \{$  $\mid x_i \in \{s, w\}\}$

$\rightsquigarrow G \times M \longrightarrow M$

$m =$  $\rightsquigarrow G_m = \{ e, (12) \} \cong \mathbb{Z}_2$

$F_{(12)}$ $\rightsquigarrow B_m = \{$  $\} \cong G/G_m \cong \mathbb{Z}_3$

$g = (12)$ $\rightsquigarrow F_{(12)} = \{$  $\}$

Bem.: $G/G_m \cong B_m$ 

Bsp. 2: G bel., $M = G$

$\rightsquigarrow G \times G \longrightarrow G$ $\qquad h \in G \rightsquigarrow G_h = \{ a \in G \mid aha^{-1} = h \}$
$= Z_h$ = Zentralisator

$(g, h) \longmapsto ghg^{-1}$ $\qquad B_h = \{ aha^{-1} \mid a \in G \}$
= Konj. Klasse

[Konjugation]

$g \in G \rightsquigarrow F_g = \{ h \in G \mid ghg^{-1} = h \}$
$= Z_g \quad \Leftrightarrow hgh^{-1} = g$ ③

③ Zählprobleme

Färbe die Ecken eines regelmäßigen Achtecks schwarz oder weiß.

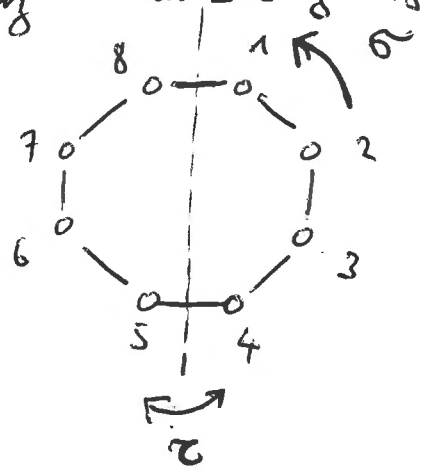
a) Wieviele Färbungen gibt es bis auf Drehungen und Spiegelungen?

ii) mit genau 4×s und 4×w. (Zusatzaufg.)

Ⓐ Math. Form.

$$G = D_8 = \langle \sigma, \tau \mid \sigma^8 = e,\ \tau^2 = e,\ \tau\circ\sigma = \sigma^{-1}\tau \rangle$$

$$M = \{ (x_1, x_2, \dots, x_8) \mid x_i \in \{\underbrace{0}_{\text{weiß}}, \underbrace{1}_{\text{schwarz}}\},\ \sum_{i=1}^{8} x_i = 4 \}$$ in Zusatzaufg.



$\rightsquigarrow D_8 \times M \longrightarrow M$

$$\sigma^i \circ (x_1, \dots, x_8) := (x_2, \dots, x_8, x_1)$$

$$\tau \circ (x_1, \dots, x_8) := (x_8, \dots, x_1)$$

$|M/_{D_8}| = \#$ gefärbte 8-Ecke bis auf Symmetrie

Bahnformel:

$$|M/_G| = \frac{1}{|G|} \sum_{g \in G} \chi(g) \qquad \chi(g) = |F_g| = |\{x \in M \mid gx = x\}|$$

- $g \sim h \Rightarrow \chi(g) = \chi(h)$

Ⓑ Konj.-Klassen in $G = D_8$

$$D_8 = \{ e;\ \sigma \sim \sigma^7,\ \sigma^2 \sim \sigma^6,\ \sigma^3 \sim \sigma^5,\ \sigma^4$$
$$\tau \sim \sigma^2\tau \sim \sigma^4\tau \sim \sigma^6\tau,\quad \sigma^8\tau = \tau$$
$$\sigma\tau \sim \sigma^3\tau \sim \sigma^5\tau \sim \sigma^7\tau \}$$

Bem.: $G = D_n \Rightarrow \sigma^i \sim \sigma^{n-i}$ $(n \geq 3)$

$\tau \sim \sigma^{2i}$ $\forall i$

$$D_{2n}/_\sim = \{ \underbrace{[e]}_{1}, \underbrace{[\sigma], \dots, [\sigma^n]}_{\text{je } 2}, \underbrace{[\tau]}_{n}, \underbrace{[\sigma\tau]}_{n} \} \qquad (n \geq 2)$$

$$\#\quad 1 \qquad \text{je } 2 \qquad 1 \qquad n \qquad n$$

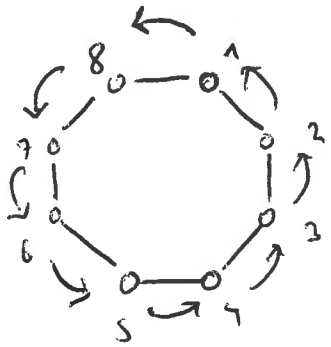
$$D_{2n+1}/_\sim = \{ \underbrace{[e]}_{1}, \underbrace{[\sigma], \dots, [\sigma^n]}_{\text{je } 2}, \underbrace{[\tau]}_{2n+1} \}$$

© Fixpunktmengen zählen

$\sum_{i=1}^{8} x_i = 4$

- $g = e$ $\quad \chi(e) = |F_e| = |M| = 2^8$ $\quad | \quad \chi(e) = |M| = \binom{8}{4} = 70.$

- $g = \sigma$. $\quad x \in F_\sigma \Leftrightarrow \sigma(x_1, \dots, x_8) = (x_1, \dots, x_8)$



$\Leftrightarrow x_1 = x_2 = \dots = x_8$ $\quad | \quad F_\sigma = \emptyset$

$\Rightarrow \chi(\sigma) = 2$ $\quad | \quad \chi(\sigma) = 0$

- $g = \sigma^2$ $\quad x \in F_{\sigma^2} \Leftrightarrow x = (x_1, x_2, x_1, x_2, \dots, x_1, x_2)$

$\Rightarrow \chi(\sigma^2) = 2^2$ $\quad | \quad \chi(\sigma^2) = 2$ [$x_1 = 1$, $x_2 = 0$ oder umgekehrt]

- $g = \sigma^3$

$x \in F_{\sigma^3} \Leftrightarrow$ ~~xxxxx~~

$x_1 = x_4 = x_7 = x_2 = x_5 = x_8 = x_3 = x_6$

$\Rightarrow \chi(\sigma^3) = 2$ $\quad | \quad \chi(\sigma^3) = 0$

- $g = \sigma^4$. $\quad x \in F_{\sigma^4} \Leftrightarrow x_1 = x_5, \dots, x_4 = x_8$

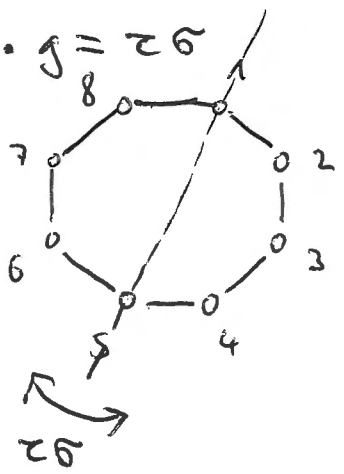
$\Rightarrow \chi(\sigma^4) = 2^4$ $\quad | \quad \chi(\sigma^4) = \binom{4}{2} = 6$

- $g = \tau$. $\quad x \in F_\tau \Leftrightarrow (x_1, \dots, x_8) = (x_8, \dots, x_1)$

$\Leftrightarrow x = (x_1, \dots, x_4, x_4, \dots, x_1)$

$\Rightarrow \chi(\tau) = 2^4$ $\quad | \quad \chi(\tau) = \binom{4}{2} = 6$

- $g = \tau\sigma$



$\tau\sigma(x_1, \dots, x_8) = (x_1, x_8, x_7, \dots, x_3, x_2)$

$x \in F_{\tau\sigma} \Leftrightarrow x = (x_1, x_2, x_3, x_4, x_5, x_4, x_3, x_2, x_1)$

$\Rightarrow \chi(\tau\sigma) = 2^5$ $\quad | \quad \chi(\tau\sigma) = 6$, denn

- falls $x_1 = x_5 = 1 \rightsquigarrow \binom{3}{1} = 3$
- $x_1 = 1$, $x_5 = 0$ $\}$ $\rightsquigarrow$ keine
- $x_1 = 0$ $\quad x_5 = 1$ $\}$
- $x_1 = x_5 = 0 \rightsquigarrow \binom{3}{2} = 3$

⑤ Bahnformel

$$|M/_{D_8}| = \frac{1}{16}\cdot\left[\chi(e) + 2\cdot[\chi(\sigma) + \chi(\sigma^2) + \chi(\sigma^3)] + \chi(\sigma^4) + 4\cdot[\chi(\tau) + \chi(\sigma\tau)]\right]$$

$$= \frac{1}{16}\left[\underset{70}{2^8} + \underset{0+2+0}{2\cdot[2+2^2+2]} + \underset{6}{2^4} + \underset{6+6}{4\cdot[2^4+2^5]}\right] = 30 = 7$$

Bem: [Konjugationsklassen berühmter Symmetriegruppen]

- $\Sigma_3 = \{e,\ (12)\sim(23)\sim(13),\ (123)\sim(132)\}$

  $\Sigma_{3/\sim} = \{[e],\ [(ab)],\ [(abc)]\}$

- $\Sigma_4 = \{[e],\ [(ab)],\ [(abc)],\ [(ab)(cd)],\ [(abcd)]\}$

  $(abc)\sim(cba)$ in Σ_4.

  $\Sigma_{n/\sim}$ analog...

- $A_4 = \{e,\ (12)(34)\sim(13)(24)\sim(14)(23),$

  $(234)\sim(143)\sim(412)\sim(321),$

  $(432)\sim(341)\sim(214)\sim(123)\}$.

  $(abc) \not\sim (cba)$!

  in A_4

Bem.: für Zählprobleme
reicht auch unvollständige Kenntnis der Konj.-Klassen.

④ Zwei Anwendungen des 2. Sylow-Satzes

Satz (Sylow 2): $|G| = m \cdot p^k$ $\quad ggT(m,p) = 1$

H eine p-UG von G $\quad$ (d.h. $|H| = p^j$ $j \le k$)

P eine p-Sylow-UG von G (d.h. $|H| = p^k$)

$\Rightarrow \exists g \in G: \; gHg^{-1} \subset P.$

Anwendungen:

1) P_1, P_2 p-Sylow-UG in G $\underbrace{\Rightarrow \exists g \in G: gP_1g^{-1} = P_2}$ $\Rightarrow P_1 \cong P_2$.

falls G abelsch $\Rightarrow P_1 = P_2$, d.h.

G hat nur eine p-Sylow-UG

Bew.:

- (S2) $\Rightarrow \exists g \in G: \; gP_1g^{-1} \subset P_2$

es gilt: $|gP_1g^{-1}| = |P_1| \underbrace{\Rightarrow}_{|P_1| = |P_2| = p^k} |gP_1g^{-1}| = |P_2|$

$\Rightarrow \quad gP_1g^{-1} = P_2$ $\square$

G abelsch: $P_1 = gg^{-1}P_1 = gP_1g^{-1} = P_2$

2) „Frattinis Argument":

Sei P p-Sylow-UG von K und $K \lhd G$

$\Rightarrow K \cdot N_G(P) = G$

Bew.: Sei $g \in G$.

$K \lhd G \Rightarrow gKg^{-1} = K$

$P \subset K \Rightarrow \underbrace{gPg^{-1}}_{\text{eine } p\text{-Sylow-UG von } K} \subset gKg^{-1} = K$

(S2) $\Rightarrow \exists k \in K: \; k \cdot \underbrace{(gPg^{-1})}_{H} k^{-1} = P$

und $H \subset K$

$\Rightarrow kg \in N_G(P) \Rightarrow g \in k^{-1} N_G(P)$ $\square$

⑤ $\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n)$

(siehe auch Aufg. 9, 11, 48, 71).

- $\mathrm{Hom}_{gr}(\mathbb{Z}_8, \mathbb{Z}_{12}) \ni \varphi \Rightarrow \varphi: \mathbb{Z}_8 \to \mathbb{Z}_{12}$

$\bar{0} \mapsto \bar{0}$

$\bar{1} \mapsto \varphi(\bar{1}) =: \bar{a}$

$\Rightarrow \varphi(\bar{k}) = \varphi(\underbrace{\bar{1}+\ldots+\bar{1}}_{k\text{-mal}}) = \underbrace{\bar{a}+\ldots+\bar{a}}_{k\text{-mal}} = k \cdot \varphi(\bar{1}) = \overline{k \cdot a}$

- $\varphi = 0 \Leftrightarrow \bar{a} = \bar{0} \Leftrightarrow a \in (12) \Leftrightarrow 8a \in (96)$
  $a \in (n)$
- φ wohldef $\Leftrightarrow \varphi(\bar{8}) = \bar{0} \Leftrightarrow \overline{8a} = \bar{0}$
  $\varphi(\bar{0})$
  $\Leftrightarrow 8a \in (12)$
  $m \cdot a \in (n)$
- $8a \in (12) = \{12, \underbrace{24}_{m \cdot n}, 36, 48, 60, 72, 84, 96, \ldots\}$

$\Leftrightarrow 8a \in (12) \cap (8) = (24) = \{24, 48, 72, 96, \ldots\}$
$m \cdot a \in (n) \cap (m) = (kgV(m,n))$

$\Leftrightarrow a \in \underbrace{(3)}_{\frac{kgV(m,n)}{m}} = (\tfrac{24}{8}) = \{3, 6, 9, 12, \ldots\} \Rightarrow \varphi(1) \in (\tilde{m})$

$\frac{kgV(m,n)}{m} = \frac{n}{ggT(m,n)} =: \tilde{m}$

$\Leftrightarrow \tilde{a} \in \{3, 6, 9, 12 = \bar{0}\}$ modulo 12

$\Rightarrow \mathrm{Hom}_g(\mathbb{Z}_8, \mathbb{Z}_{12}) \xrightarrow{\sim} \mathbb{Z}_4$

$\varphi \mapsto \frac{\varphi(1)}{3}$

$(\bar{1} \mapsto 3 \cdot \bar{d}) \longleftarrow \bar{d}$

$\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) \xrightarrow{\sim} \mathbb{Z}_{ggT(m,n)}$

$\varphi \mapsto \varphi(\bar{1}) \cdot \frac{ggT(m,n)}{n}$

$(\bar{1} \mapsto \frac{n}{ggT(m,n)} \cdot \bar{d}) \longleftarrow \bar{d}$

Bem.: i) $\mathrm{Hom}_{\text{Rings}}(\mathbb{Z}_8, \mathbb{Z}_{12}) = \{\varphi\}$

$\varphi: \bar{0} \mapsto \bar{0}$

$\bar{1} \mapsto \bar{1}$

$\Rightarrow \bar{8} = \bar{0} \mapsto \bar{8} \neq \bar{0}$ ↯

ii) $\mathbb{Z}_{12} \xrightarrow[\text{[ERS]}]{\sim} \mathbb{Z}_3 \times \mathbb{Z}_4$

$\Rightarrow \mathrm{Hom}(\mathbb{Z}_8, \mathbb{Z}_{12}) \cong \overbrace{\mathrm{Hom}(\mathbb{Z}_8, \mathbb{Z}_3)}^{0} \times \underbrace{\mathrm{Hom}(\mathbb{Z}_8, \mathbb{Z}_4)}_{\cong \mathbb{Z}_4}$

⑥ $x^e \equiv y \bmod n$ und RSA-Verfahren

$\mathbb{Z}_n^* =$ Gruppe der Einheiten von $(\mathbb{Z}_n, \cdot)$

Lemma: $\forall a \in \mathbb{Z}$: $\bar{a} \in \mathbb{Z}_n^* \Leftrightarrow ggT(a,n) = 1$

$\Leftrightarrow$ „$\bar{a}$ invertierbar in $\mathbb{Z}_n$"

Bsp.: $\mathbb{Z}_9^* = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}\}$ $\quad \varphi(9) = 6$

Def.: $\varphi(n) = |\mathbb{Z}_n^*| = |\{1 \le a < n \mid ggT(a,n) = 1\}|$ Euler'sche φ-Funktion

Satz (Euler): $ggT(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$

[folgt aus Lemma und weil $\operatorname{ord} a \mid \varphi(n)$]

Kor.: $n = p$ prim, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \bmod p$ $\quad \varphi(p) = p-1$

Aufg. 1: Löse $x^{25} \equiv 9 \bmod 35$. $\quad 35 = 5 \cdot 7$, $ggT(25, \varphi(35)) = 1$.

- $\varphi(35) = |\mathbb{Z}_{35}^*| = |\mathbb{Z}_5^* \times \mathbb{Z}_7^*| = 4 \cdot 6 = 24$
- $ggT(9,35) = 1 \Rightarrow 9 \in \mathbb{Z}_{35}^* \Rightarrow x^{25} \in \mathbb{Z}_{35}^*$

$\Rightarrow ggT(x^{25}, 35) = 1 \Rightarrow ggT(x, 35) = 1$.

$\overset{\text{Satz}}{\Rightarrow} x^{24} \equiv 1 \bmod 35 \Rightarrow \underbrace{x \cdot x^{24}}_{x^{25}} \equiv 9 \bmod 35$.

$\Rightarrow$ genau eine Lösung mod n.

Aufg. 2: Löse $x^{25} \equiv 9 \bmod 36$ $\quad 36 = 3^2 \cdot 2^2$

- $\mathbb{Z}_{36} \xrightarrow[\text{[CRS]}]{\sim} \mathbb{Z}_9 \times \mathbb{Z}_4 \Rightarrow \varphi(36) = \varphi(9) \cdot \varphi(4) = 6 \cdot 2 = 12$

$ggT(12, 36) \neq 1, \ldots$

$$x^{25} \equiv 9 \bmod 36 \overset{\text{[CRS]}}{\Leftrightarrow} \begin{cases} x^{25} \equiv 9 \bmod 9 \\ x^{25} \equiv 9 \bmod 4 \end{cases} \Leftrightarrow \begin{cases} 9 \mid x^{25} \\ x^{25} \equiv 1 \bmod 4 \end{cases}$$

- $ggT(1,4) = 1 \Rightarrow ggT(x^{25}, 4) = 1 \Rightarrow ggT(x, 4) = 1$

$\varphi(4) = 2 \overset{\text{Satz}}{\Rightarrow} x^2 \equiv 1 \bmod 4 \Rightarrow x^{25} \equiv x \equiv 1 \bmod 4$

$$x^{25} \equiv 9 \bmod 36 \iff \begin{cases} 9 \mid x^{25} \\ x \equiv 1 \bmod 4 \end{cases} \iff \begin{cases} 3 \mid x \\ x \equiv 1 \bmod 4 \end{cases}$$

$\Rightarrow \overline{x} \in \{\overline{9}, \overline{21}, \overline{33}\}$ modulo 36.

$\rightsquigarrow$ 3 Lösungen mod n.

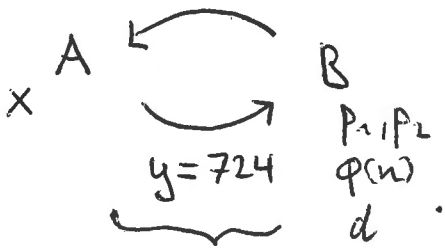
Aufg. 3: $x^2 \equiv 3 \bmod 4$ $\rightsquigarrow$ keine Lösung.

Lemma: Seien $n = \underbrace{p_1 \cdot \ldots \cdot p_t}_{\text{verschiedene Primzahlen}}$, $e \in \mathbb{N}$ mit $\underbrace{ggT(e, \varphi(n)) = 1}_{\exists e^{-1} \in \mathbb{Z}_{\varphi(n)}}$ und $y \in \mathbb{N}$. Dann hat $x^e \equiv y \bmod n$ die eindeutige Lsg.: $x \equiv y^d \bmod n$, wobei $d \equiv e^{-1} \bmod \varphi(n)$ bzw. $d \cdot e + l \cdot \varphi(n) = 1$ für ein $l \in \mathbb{Z}$.

Anwendung: RSA-Verfahren

- A will B x sagen, aber E hört mit
- B wählt p_1, p_2 $\rightsquigarrow$ $n = \boxed{p_1}\boxed{p_2} = 9.991$
  mit $p_1 \neq p_2$ $\rightsquigarrow$ $\boxed{\varphi(n)} = (p_1 - 1) \cdot (p_2 - 1)$
  $\rightsquigarrow$ $e = 11$ erfüllt $ggT(e, \varphi(n)) = 1$

(9.991, 11) = (n, e)



- A rechnet $\boxed{x}^e$ mod n aus
  $\rightsquigarrow \boxed{x}^e \equiv y \bmod n$ $\quad y = 724$
- E sieht nur $x^{11} \equiv 724 \bmod 9.991$

E sieht das

- B rechnet $\boxed{d}$ aus, und y^d

$ggT(e, \varphi(n)) = 1 \Rightarrow \exists d, l \in \mathbb{Z}: \; d \cdot e + l \cdot \varphi(n) = 1$

Euklid. Alg.

$\Rightarrow \boxed{x} \equiv y^{\boxed{d}} \bmod n$

Lemma

Aufg.*: Was ist x ?

Ansatz [Fermat-Faktorisierung]:

$n = a^2 - b^2 = (a-b)\cdot(a+b)$ ⇝ suche a und b.

$9.991 = 10.000 - 9 = 100^2 - 3^2 = (100-3)(100+3)$

$= 97 \cdot 103$

$\Rightarrow p_1 = 97 \quad p_2 = 103 \Rightarrow n = 9.991$ ist unsicher!

$\Rightarrow \varphi(n) = (p_1-1)\cdot(p_2-1) = 96 \cdot 102 = 9.792$

$e = 11$ ✗ 9.792, denn

$\left.\begin{aligned} 9.792 &= 890 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 + 1 \end{aligned}\right\}$ $1 = 11 - 5\cdot(9.792 - 890\cdot 11)$

$= 4451 \cdot 11 - 5 \cdot 9.792$

$1 = d \cdot e + \ell \cdot \varphi(n)$

$\Rightarrow d = 4451 \Rightarrow x \equiv 724^{4451} \bmod 9.991$

⇝ E berechnet $724^{4451} \equiv 42 \bmod 9.991$

$\Rightarrow x = 42.$

⑦ Zwei Bemerkungen zu Polynomen

Lemma: $f \in K[X]$.

f irreduzibel $\Leftrightarrow$ (f) maximales Ideal $\Leftrightarrow$ $K[X]/(f)$ ein Körper

Bew.: „$\Rightarrow$": Sei f irred. Sei $(f) \subseteq I \subseteq K[X]$. ($I$ Ideal)

Beh.: $I = (f)$ oder $I = K[X]$.

- ~~K[X] K[X]~~

$K[X]$ ein Hauptidealring $\Rightarrow \exists g \in K[X]: I = (g)$

$(f) \subseteq (g) \Rightarrow f \in (g) \Rightarrow \exists h \in K[X]: f = hg$

f irreduzibel $\Rightarrow h \in K^*$ oder $g \in K^*$

$\Rightarrow g = h^{-1} f$ oder $(g) = (g^{-1} \cdot g) = (1) = K[X]$

$\Rightarrow (g) = (h^{-1} f) = (f)$ oder $(g) = K[X]$.

„$\Leftarrow$": (f) maximal. Beh.: f irred.

Sei $f = g \cdot h \Rightarrow (f) \subseteq (g) \Rightarrow (f) = (g)$ oder $(g) = K[X]$
((f) max.)

$\Rightarrow h \in K^*$ oder $g \in K^*$. □

Bsp.: $K = \mathbb{Q} \subset L = \mathbb{C}$ $\alpha = \sqrt[4]{2} \in L$

Beh.: $f(x) = x^4 - 2$ ist Min. Polynom von α

Bew.: f Min. Pol. von $\alpha \Leftrightarrow$
- f normiert ✓
- $f(\alpha) = 0$ ✓
- und f irreduzibel ✓ [nach Eisenstein].

Bem.: $\mathbb{Q}(\sqrt[4]{2})$ ist kein Zerfällungskörper von

$f(x) = x^4 - 2$,

denn $\mathbb{Q}(\sqrt[4]{2})$ enthält nicht alle Nullstellen von f in $\mathbb{C}$.

$\pm\sqrt[4]{2}, \pm\sqrt[4]{2}\,i$.