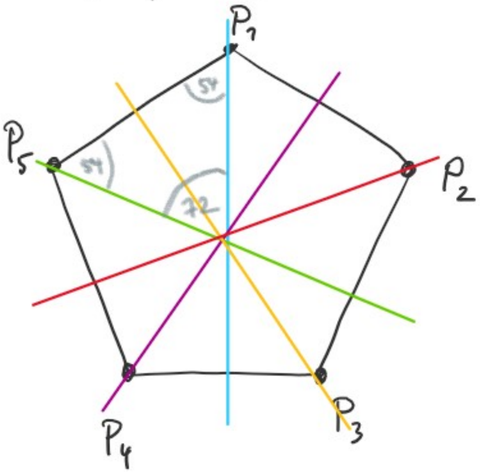
24.01.16

Freitag, 12. Januar 2024 11:34

Die Diedergruppe

Die Diedergruppe D_5 besteht aus 10 Elementen, den Isometrien des regulären 5eck. Das sind Drehungen und Spiegelungen wie folgt: $D_5 := \{0, 1, 2, \ldots, 9\}$



Für $k \in \{0, \ldots, 4\}$

$k :=$ Drehung um $k \cdot 72°$ gegen den Uhrzeigersinn

$k \in \{5, 6, 7, 8, 9\}$ = Spiegelung an Geraden durch:

P_1, P_3, P_5, P_2, P_4

Die Verknüpfung $*$ ist die Hintereinanderausführung zweier Isometrien, also

z.B. $5 * 1$ = Spiegelung an P_1 <u>nach</u> Drehung um $72°$.

Man beobachtet: $5 * 1 = \overbrace{1^4}^{= 1*1*1*1} * 5$ denn

$P_1 \xmapsto{1} P_5 \xmapsto{5} P_2$ $\qquad$ $P_1 \xmapsto{5} P_1 \xmapsto{1^4} P_2$

$P_2 \xmapsto{1} P_1 \xmapsto{5} P_1$ $\qquad$ $P_2 \xmapsto{5} P_5 \xmapsto{1^4} P_1$

$P_2 \xmapsto{1} P_1 \xmapsto{5} P_1$ $\qquad$ $P_2 \xmapsto{5} P_5 \xmapsto{1^4} P_1$

$P_3 \xmapsto{1} P_2 \xmapsto{5} P_5$ $\qquad$ $P_3 \xmapsto{5} P_4 \xmapsto{1^4} P_5$

$P_4 \xmapsto{1} P_3 \xmapsto{5} P_4$ $\qquad$ $P_4 \xmapsto{5} P_3 \xmapsto{1^4} P_4$

$P_5 \xmapsto{1} P_4 \xmapsto{5} P_3$ $\qquad$ $P_5 \xmapsto{5} P_2 \xmapsto{1^4} P_2$

Damit kann man folgende Verknüpfungstabelle aufstellen:

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

Satz 181 $(D_5, *)$ bildet eine Gruppe.

Beweis Abgeschlossenheit von $*$, also: aus $g, h \in D_5 \Rightarrow g * h \in D_5$ sieht man an der Tabelle.

Assoziativität: klar wegen Hintereinanderausführung von Abbildungen.

Neutrales Element $= 0 =$ Drehung um $0°$

Inverses Element einer Spiegelung ist die Spiegelung selbst, einer Drehung um α eine Drehung um $360° - \alpha$. (sieht man auch an der Tabelle) $\square$

Man betrachtet folgende Permutationen $\pi_1, \ldots, \pi_n$:

$$\pi_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix}$$

$$\pi_k := \underbrace{\pi_1 \circ \cdots \circ \pi_1}_{k\text{-mal}} : D_5 \to D_5$$

z.B. π_2:

	0	1	2	3	4	5	6	7	8	9
π_1	1	5	7	6	2	8	3	0	9	4
π_2	5	8	0	3	7	9	6	1	4	2

Der DM-Code

Beispiel 182 1) Es kommen 10 Buchstaben vor die durch Zahlen ersetzt werden:

A	D	G	K	L	N	S	U	V	Z
0	1	2	3	4	5	6	7	8	9

2) Bestimmung der Prüfziffer mit Kontrollsymbol $c = 0$, $n = 11$ und $\pi_n = \mathrm{id}$

$$\pi_1(g_1) * \cdots * \pi_{10}(g_{10}) * \overbrace{\pi_{11}(g_{11})}^{= g_{11}} = 0$$

$$\Rightarrow \quad g_{11} = \left(\pi_1(g_1) * \cdots * \pi_{10}(g_{10})\right)^{-1}$$

Als Beispiel sei AU1210706Z eine Geldscheinnummer. Ohne Buchstaben ergibt das

0 7 1 2 1 0 7 0 6 9 . Man berechnet: $\pi_1(0) = 1$, $\pi_2(7) = 1$, $\pi_3(1) = 9$, ..., $\pi_{10}(9) = 2$ und daraus

$$g_{11}^{-1} = 1 * 1 * 9 * 5 * 2 * 2 * 2 * 0 * 3 * 2 = 2$$

$$\Rightarrow \quad g_{11} = 3$$

Somit ist die Geldscheinnummer mit Prüfziffer gleich A Y 1 2 1 0 7 0 6 Z 3

3) Erfüllt der Code die Anforderungen? Nach Satz werden alle Einzelfehler erkannt. Dass Vertauschungen erkannt werden muss für alle Elemente und Permutationen nachgerechnet werden. Die letzten beiden Stellen werden bei einer Vertauschung immer erkannt da die vorletzte Stelle eine Ziffer und die letzte Stelle ein Buchstabe ist.

Kryptologie

ist die Wissenschaft, die sich mit Ver- und Entschlüsselung von Informationen (und somit der Informationssicherheit) beschäftigt. Arbeits-

Informationssicherheit) beschäftigt. Arbeitsfelder sind: 1) Verschlüsselungsverfahren
2) digitale Signaturen = Authentifizierung

Man unterteilt die Kryptologie in

Krypographie → symmetrische Kryptographie, Public-Key Kryptographie

Kryptoanalyse → Sicherheitsanalyse von Vofahren

Ver- und Entschlüsselung von Informationen dient dazu, Nachrichten zu übertragen ohne dass Dritte die Informationen abfangen können.

Symmetrisches Verschlüsselungsverfahren

Klartext → Geheimtext

Senter verschlüsselt den Klartext mit ==Schlüssel S==

Sender verschickt Geheimtext, ggf. Angriff Dritter

Klartext ← Geheimtext

Klartext $\longleftarrow$ Geheimtext

Empfänger entschlüsselt mit Schlüssel S

Asymmetrische / Public-Key - Verfahren

Der Empfänger generiert einen öffentlichen und einen privaten Schlüssel. Der öffentliche Schlüssel wird bekannt gegeben:

Klartext $\longrightarrow$ Geheimtext

Sender verschlüsselt mit öffentlichem Schlüssel $S_ö$ des Empfängers

Sender verschickt Geheimtext, ggf. Angriff Dritter

Klartext $\longleftarrow$ Geheimtext

Empfänger entschlüsselt mit seinem privaten Schlüssel S_p

Public-Key - Verschlüsselung

<u>Allgemeines Verfahren</u>: jeder Teilnehmer T besitzt einen öffentlichen Schlüssel E_T und einen priva-

itzt einen öffentlichen Schlüssel E_T und einen priva-
ten Schlüssel D_T mit den Eigenschaften

a) Entschlüsselungseigenschaft: Für jede Nachricht m gilt $D_T(\underbrace{E_T(m)})=m$

$\underbrace{E_T(m)}$ = Geheimtext: m wird mit E_T verschlüsselt

D_T: Entschlüsselung mit D_T

b) Public-Key-Eigenschaft: D_T kann aus E_T praktisch nicht ermittelt werden.

<u>Vorteil</u> die geheimen Schlüssel müssen nicht übertragen / ausgetauscht werden. Eignet sich gut für mehrere Teilnehmenden.

Möchte man nicht verschlüsselte Informationen übertragen, sondern einen Sender authentifizieren so müssen D_T und E_T die

a') Authentifizierungseigenschaft: $E_T(D_T(m))=m$ für alle Nachrichten m haben.

Das Verfahren läuft dann so:

Sender: → verschlüsselt Nachricht m zu $D_T(m)$

→ schickt m und $D_T(m)$

Empfänger → entschlüsselt $D_T(m)$ zu $E_T(D_T(m))$

und vergleicht mit m

Signierung / Authentifizierung

Sender: s1) Mail + Anlage werden mit einem

D_T, E_T
privat öffentlich

Einmalkennwort verschlüsselt

s2) Kennwort wird mit Public key des
m

$E_{T'}(m)$

Empfängers verschlüsselt

$D_T(s)$

s3) Prüfsumme der Mail wird mit
s

dem eigenen privaten Schlüssel verschlüs

s, $D_T(s)$

$E_{T'}(m)$

-selt

Empfänger e1) prüft s3) mit dem Public key des

$D_{T'}$, $E_{T'}$
↑ ↑
privat öffentlich

Senders $E_T(D_T(s)) = s$

e2) entschlüsselt Einmalkennwort mit

seinem privaten Schlüssel $D_{T'}(E_{T'}(m)) = m$

seinem privaten Schlüssel $D_{T'}(E_{T'}(m)) = m$

e3) decodiert die Mail mit Kennwort

aus e2)

RSA - Verfahren (Rivest, Shamir, Adleman 1978)

Grundlage für die Sicherheit des Verfahrens: für sehr große Primzahlen p, q, $p \neq q$ ist es leicht $n = p \cdot q$ zu berechnen. Aber aus vorgelegtem $n \in \mathbb{N}$ ist es <u>sehr</u> <u>aufwändig</u> die Primfaktoren p, q mit $n = p \cdot q$ zu berechnen.

Satz 183 (kleiner Satz von Fermat)

Für $m \in \mathbb{N}$ und p Primzahl gilt: $m^p \equiv m \mod p$

(bzw: $m^{p-1} \equiv 1 \mod p$)

Beweis Aus UEB ? wissen wir $(x+y)^p \equiv x^p + y^p \mod p$. Mit Induktion über m:

<u>$m = 1$</u>: $1^p \equiv 1 \mod p$

<u>$m \mapsto m+1$</u> $(m+1)^p \equiv m^p + 1^p \overset{IV}{\equiv} m + 1 \mod p$ $\square$