

3. Aufgabenblatt

KRYPTOGRAPHIE (für GHRG) (SS 2011)

Abgabe: Freitag 29.4.2011, bis 9.15 Uhr

Gruppen 1 und 2 (Mo): Fach Nr. 3 (orangener Schrank bei D1.348)

Gruppen 3 und 4 (Do): Fach Nr. 11 (orangener Schrank bei D1.348)

Internet: <http://math-www.uni-paderborn.de/~chris>

Schreiben Sie bitte auf die erste Seite **gut** leserlich Namen, Vornamen, Matrikel-Nr. und Nr. Ihrer Übungsgruppe. Heften Sie bitte die Seiten zusammen!

Es können **Bonuspunkte** für die Leistungsnachweis-Klausur erworben werden.

Es ist nur Einzelabgabe erlaubt. **Es sind immer Begründungen erforderlich!**

7. Aufgabe: a) Liste alle möglichen Abbildungen $\{a, b, c\} \longrightarrow \{1, 2, 3\}$ auf. Wieviele gibt es? Wieviele davon sind injektiv, surjektiv, bijektiv, weder injektiv noch surjektiv?

b) Bestimme die Anzahl aller injektiven Abbildungen $\{1, 2, 3, 4, 5\} \longrightarrow \{3, 4, 5, 6, 7, 8, 9, 10\}$.

c) Finde eine Formel für die Anzahl aller injektiven Abbildungen von einer m -elementigen Menge M in eine n -elementige Menge N . Begründe! (5)

8. Aufgabe: $f, g : M \longrightarrow N$ und $h : N \longrightarrow P$ seien Abbildungen.

a) Beweise: Ist h injektiv und gilt $h \circ f = h \circ g$, so folgt $f = g$.

b) Untersuche, ob die Aussage in a) auch richtig bleibt, wenn h nicht injektiv ist (gib entweder einen allgemeinen Beweis oder gib ein konkretes Gegenbeispiel an). (3)

9. Aufgabe: Beweise: $V_A^{-1} \circ V_G = V_U^{-1} \circ V_A$. (2)

Fortsetzung nächste Seite!

10. Aufgabe: Entschlüssele den folgenden Geheimtext, beschreibe dein Vorgehen und schreibe den Klartext lesbar auf:

UIZTMAVRLHMRISZHRGNZNZVSIRGQFRGTHMRGDVREVRORLHMRIRVRISZ

HMAFSRFMRHXSLGYRNZOMDRVHHGVXSMZGMDLIMRMAVRHRIPRGGRALXSG

LXSPRVGRYVQRPMVERGZYYVOAFGTRG

Hinweis: Dieser Geheimtext ist nicht durch eine Verschiebechiffre verschlüsselt worden, sondern durch irgendeine bijektive Abbildung $f : \mathfrak{A} \rightarrow \mathfrak{A}$. Beim Entschlüsseln könnte es hilfreich sein, nicht nur die Häufigkeiten einzelner Buchstaben zu untersuchen, sondern auch die Häufigkeiten von Buchstabenpaaren. (8)

Achtung!

Schreibe auf die erste Seite deiner Bearbeitung oben rechts eine Punktetabelle der Form

7	8	9	10	Σ

in die die Korrektorinnen die Punkte eintragen können. Verfahre bei den folgenden Übungen entsprechend!

Rücksprache!

Wenn du eine der Korrektorinnen wegen der Korrektur sprechen möchtest, schreibe eine email an

Name	Kürzel	email-Adresse
Natalie Benke	NB	natka@mail.uni-paderborn.de
Andrea Bröcker	AB	andrea.broecker@gmail.com
Daniela Wullenweber	DW	Daniela.Wullenweber@web.de

Frohe Ostern!