. . . . . .
1. Name und Matrikel-Nummer

. . . . . .
2. Name und Matrikel-Nummer

. . . . . .
Gruppe

Lineare Algebra I – Blatt 5

hhu Düsseldorf, WiSe 2019/20

1	2	3	4	Σ

Abgabe: bis Mittwoch 13.11.2019 bis 10:15 Uhr, in den Briefkästen

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~internet/LAI_WS1920/`
Bitte drucken Sie diese Seite aus und verwenden Sie sie als Deckblatt für Ihre Lösungen.
Wie üblich sind alle Behauptungen zu beweisen. Wenn Sie Resultate aus der Vorlesung verwenden, geben Sie bitte die zugehörigen Referenznummern mit an.

Aufgabe 1 (4 Punkte):

Sei $(G, +)$ eine kommutative Gruppe und U eine Teilmenge von G, die bezüglich $+$ auch eine Gruppe ist (eine sogenannte Untergruppe von G). Jede Untergruppe U enthält 0 und mit $u \in U$ ist auch $-u \in U$. (Das dürfen Sie verwenden, ohne es zu zeigen.)

(a) Zeigen Sie, dass durch $x \sim y :\Leftrightarrow x - y \in U$ eine Äquivalenzrelation auf G definiert wird und die Mengen $x + U := \{x + u;\ u \in U\}$ die Äquivalenzklassen $[x]$ bezüglich $\sim$ sind.

(b) Zeigen Sie, dass die Quotientenmenge $G/\sim$ durch die naheliegende Definition von "$+$" mit den Repräsentanten x, y von $[x], [y] \in G/\sim$ wieder eine kommutative Gruppe wird.

Aufgabe 2 (4 Punkte):

Schreiben Sie die folgenden komplexen Zahlen in der Form $x + iy$ mit $x, y \in \mathbb{R}$, wobei $i^2 = -1$. Berechnen Sie auch jeweils deren multiplikative Inverse und Quadrat in dieser Form, sowie deren Betrag.

$$z_1 := \frac{1}{1-i}, \qquad z_2 := \frac{1-i}{1+i}, \qquad z_3 := \frac{(1+2i)^2}{2+3i}, \qquad z_4 := \left(\frac{4-i}{2+i}\right)^2.$$

Aufgabe 3 (4 Punkte):

Führen Sie die folgenden Polynomdivisionen aus.

(a) $(T^5 - 2T^3 + T - 4) : (T - 2)$ (b) $(T^4 + T^2 + 1) : (T^2 + T + 1)$

Wie lautet von dem Polynom $P := T^4 + T^2 + 1$ die Faktorisierung in Linearfaktoren über $\mathbb{C}$?

Aufgabe 4 (4 Punkte):

Welche der folgenden Mengen sind Untervektorräume des Vektorraums $\mathbb{R}[T]$ der reellen Polynome in einer Unbestimmten T?

(a) $\{f \in \mathbb{R}[T];\ \deg f \geq 2 \vee f = 0\}$,

(b) $\{f \in \mathbb{R}[T];\ f(0) = 0\}$,

(c) $\{f \in \mathbb{R}[T];\ f = \sum_{i=0}^{n} \alpha_i T^i, n \in \mathbb{N}_0$ beliebig, mit $\alpha_j = 0$ falls j ungerade$\}$.

Bitte wenden

Wissensfragen zu L8 und L9: (nur mündlich, ohne Abgabe)

1.) Kann man die Zahlbereiche $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ mithilfe von Äquivalenzrelationen konstruieren?

2.) Wie kann man den Körper $\mathbb{C}$ als Fortsetzung des Körpers $\mathbb{R}$ der reellen Zahlen erhalten?

3.) Sind $\mathbb{R}$ und $\mathbb{C}$ angeordnete Körper?

4.) Wann nennt man zwei Körper isomorph?

5.) Was ist die konjugiert komplexe Zahl zu einer komplexen Zahl z? Was ist ihr Absolutbetrag?

6.) Was ist ein Polynom über einem Körper K (in einer Unbestimmten)?

7.) Wie definiert man die Addition und Multiplikation zweier Polynome?

8.) Wie lautet der Satz von der Polynomdivision?

9.) Was ist eine Nullstelle eines Polynoms?

10.) Wann kann man einen Linearfaktor von einem Polynom abspalten?

11.) Wie lautet der Fundamentalsatz der Algebra?

12.) Welche andere mögliche Konstruktion von $\mathbb{C}$ kann man mit Hilfe einer Äquivalenzrelation vornehmen?

13.) Was ist ein Vektorraum über einem Körper K?

14.) Was ist die Addition und die Skalarmultiplikation eines Vektorraums?

15.) Welche Beispiele für einen Vektorraum kennen Sie?

16.) Welche (Rechen-)Eigenschaften haben Vektorräume?

17.) Was ist ein Untervektorraum? Was ist ein affiner Unterraum?

18.) Ist der Schnitt und die Vereinigung von Vektorräumen wieder ein Vektorraum?

19.) Was ist die Summe zweier Untervektorräume?

20.) Was ist eine Linearkombination einer endlichen Familie von Vektoren eines Vektorraums?

21.) Was ist die lineare Hülle einer Teilmenge S eines Vektorraums? Welche Eigenschaften hat diese?

22.) Wann nennt man eine Teilmenge S eines Vektorraums V ein Erzeugendensystem eines Untervektorraums U von V?

Kreative Aufgabe (ohne Abgabe, keine Besprechung):

In dem Restklassenring $\mathbb{Z}/M$ gelten auch die Potenzgesetze $\bar{x}^{a+b} = \bar{x}^a \bar{x}^b$ und $(\bar{x}^a)^b = \bar{x}^{ab}$ für $a, b \in \mathbb{N}_0$. Anwendung: Alice denkt sich eine zufällig gewählte geheime natürliche Zahl a aus, und Bob ebenso eine geheime Zahl b. Alice berechnet die Restklasse $\bar{x}^a$ und sendet das Ergebnis an Bob, und Bob berechnet die Restklasse $\bar{x}^b$ und sendet das Ergebnis an Alice. Nach diesem Austausch berechnet Alice das Geheimnis $\bar{s} = (\bar{x}^b)^a = \bar{x}^{ab}$ und Bob berechnet $\bar{s} = (\bar{x}^a)^b = \bar{x}^{ab}$, was dasselbe ist. Alice und Bob haben sich auf diesem Wege auf ein gemeinsames Geheimnis geeinigt, ohne es jemals ausgetauscht zu haben! Ein Beobachter der Kommunikation hingegen verfolgt nur den Austausch von $\bar{x}^a$ und $\bar{x}^b$, kann aber nicht oder nur sehr schwer auf das Geheimnis $\bar{x}^{ab}$ kommen. Stimmt das? Wie müssen M und die Basis $\bar{x}$ idealerweise gewählt werden, damit die Geheimnisvereinbarung gelingt und sicher vor Beobachtern ist?