

3. Übung zur Algebra

Dr. L. Iancu, WiSe 2020

Aufgabe 1. Sei G eine Gruppe. Gegeben seien $g_1, g_2 \in G$ mit $o(g_1) < \infty$ und $o(g_2) < \infty$. Zeigen Sie: Gilt $g_1g_2 = g_2g_1$ und $\text{ggT}(o(g_1), o(g_2)) = 1$, so folgt $o(g_1g_2) = o(g_1)o(g_2)$.

Geben Sie Beispiele an, die zeigen, dass man auf keine der beiden Voraussetzungen verzichten kann.

Aufgabe 2. (Schriftlich 7 Punkte) Sei $n \geq 2$. Eine Permutation $\pi \in S_{n-1}$ können wir auch als Permutation von S_n auffassen, indem wir $\pi(n) = n$ setzen. Damit ist also $S_{n-1} \leq S_n$. (Ist $\pi \in S_n$ und $\pi(n) = n$, so können wir umgekehrt π auch als Permutation in S_{n-1} auffassen.)

(a) Für $1 \leq k < n$ sei $\tau_k \in S_n$ die Permutation mit $\tau_k(k) = n$, $\tau_k(n) = k$ und $\tau_k(j) = j$ für $j \in \{1, \dots, n\} \setminus \{k, n\}$, d.h., τ_k vertauscht k und n und lässt alle anderen Ziffern fest. Zeigen Sie, dass $\{\text{id}, \tau_1, \dots, \tau_{n-1}\}$ ein Repräsentantensystem für die (Links-)Nebenklassen von S_{n-1} in S_n ist, d.h., es gilt $S_n = S_{n-1} \cup \tau_1 S_{n-1} \cup \dots \cup \tau_{n-1} S_{n-1}$, wobei die Vereinigung disjunkt ist.

(b) In S_4 finden Sie die Linksnebenklasse und die Rechtsnebenklasse von τ_2 bezüglich S_3 .

[Hinweis zu (a): Wegen $|S_n| = n!$ und $|S_{n-1}| = (n-1)!$ ist nach dem Satz von Lagrange klar, dass es genau n Nebenklassen in S_n bezüglich S_{n-1} gibt. Sei nun $\pi \in S_n$ beliebig und setze $k := \pi(n)$. Ist $k = n$, so gilt bereits $\pi \in S_{n-1}$; ist $k < n$, so betrachte $\tau_k \circ \pi$.]

Aufgabe 3. Sei G eine Gruppe, H eine Untergruppe von G und $a, b \in G$. Wahr oder falsch (mit Beweis oder Gegenbeispiel) :

(a) Wenn $aH = bH$ dann $Ha = Hb$.

(b) Wenn $Ha = Hb$, dann $b \in Ha$.

(c) Wenn $aH = bH$, dann $Ha^{-1} = Hb^{-1}$.

(d) Wenn $aH = bH$, dann $a^2H = b^2H$.

Aufgabe 4. (Schriftlich, 9 Punkte) (a) Gegeben seien $a, b, m \in \mathbb{Z}$ mit $a \neq 0$ und $m > 0$. Zeigen Sie: Genau dann gibt es ein $x \in \mathbb{Z}$ mit $ax \equiv b \pmod{m}$, wenn $\text{ggT}(a, m)$ ein Teiler von b ist.

(b) Für jede der folgenden Kongruenzgleichungen, finden Sie entweder alle Lösungen $x \in \mathbb{Z}$, oder zeigen Sie, dass keine Lösung existiert.

$$\begin{aligned} 99x &\equiv 18 \pmod{30}, & 91x &\equiv 84 \pmod{143}, & x^2 &\equiv 2 \pmod{5}, \\ x^2 &\equiv 1 \pmod{8}, & x^2 + x + 1 &\equiv 0 \pmod{5}, & x^2 + x + 1 &\equiv 0 \pmod{7}. \end{aligned}$$

Aufgabe 5. Sei $n \in \mathbb{N}$ und $\Phi(n)$ die Eulersche Phi-Funktion.

(a) Sei $n = 2^k$ mit $k \geq 1$. Bestimmen Sie $\phi(n)$.

(b) Bestimmen Sie alle $n \in \mathbb{N}$ mit $\phi(n) \leq 2$. Zum Beispiel gilt $\phi(1) = \phi(2) = 1$, $\phi(3) = \phi(4) = \phi(6) = 2$. Gibt es noch weitere solche n ?

[*Hinweis zu (b):* Sei $n \geq 7$. Dann sind 1 und $n-1$ teilerfremd zu n , also ist $\phi(n) \geq 2$. Ist n ungerade, so betrachte auch $n-2$. Ist n gerade, so schreibe $n = 2^k m$ mit $k \geq 1$ und $m \in \mathbb{N}$ ungerade. Ist $m = 1$, siehe Teil (a); ist $m = 3$, betrachte $1, 7, n-1$. Ist $m \geq 5$, so betrachte $m-2$. Oder verwenden Sie die allgemeine Formel aus der folgenden Aufgabe.]

Aufgabe 6. (Zum Selbststudium) Es soll eine allgemeine Formel für die Eulersche Phi-Funktion hergeleitet werden. Für $a, b \in \mathbb{Z}$ mit $a < b$ bezeichnen wir $[a, b) := \{m \in \mathbb{Z} \mid a \leq m < b\}$ (nicht zu verwechseln mit den Bezeichnungen in der Analysis). Für $n \in \mathbb{N}$ ist dann also $\phi(n)$ nach Definition die Anzahl der zu n teilerfremden Zahlen im Intervall $[0, n)$.

(a) Zeigen Sie: Für jedes $k \in \mathbb{N}$ ist $\phi(n)$ auch die Anzahl der zu n teilerfremden Zahlen im Intervall $[kn, (k+1)n)$.

(b) Sei $n \in \mathbb{N}$ und p eine Primzahl. Zeigen Sie:
$$\phi(pn) = \begin{cases} p\phi(n) & \text{falls } p \mid n, \\ (p-1)\phi(n) & \text{falls } p \nmid n. \end{cases}$$

[*Hinweis:* Zerlegen Sie das gesamte Intervall $[0, pn)$ in die Teilintervalle $[0, n)$, $[n, 2n)$, \dots , $[(p-1)n, pn)$. Ist $k \in \mathbb{N}_0$ in einem dieser Teilintervalle, wie hängen dann die Bedingungen $\text{ggT}(k, n) = 1$ und $\text{ggT}(k, pn) = 1$ voneinander ab? Dazu wird die Unterscheidung der beiden Fälle $p \mid n$ und $p \nmid n$ wichtig sein.]

(c) Sei nun $n \in \mathbb{N}$, $n \geq 2$, und schreibe $n = p_1^{n_1} \cdots p_r^{n_r}$ mit paarweise verschiedenen Primzahlen p_1, \dots, p_r und $n_i \in \mathbb{N}$ für $1 \leq i \leq r$. Benutzen Sie dann (b), um zu zeigen:

$$\phi(n) = \prod_{i=1}^r p_i^{n_i-1} (p_i - 1) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

Bemerkung: Der obige, sehr elementare Beweis für die Formel in (c) ist entnommen aus:

S. CHORGE AND J. VARGAS, Proof of Euler's ϕ (Phi) Function Formula, Rose-Hulman Undergraduate Mathematical Journal **14** (2013), Article 6.

(Online verfügbar auf <https://scholar.rose-hulman.edu/rhumj/vol14/iss2/6>.) Für einen völlig anderen Beweis (der vielleicht etwas kürzer ist, aber dafür auch etwas mehr allgemeine Theorie benötigt) siehe zum Beispiel §6.3.3 im Buch von Karpfinger–Meyberg.

Abgabe der schriftlichen Aufgaben: Bis Mittwoch, den 18.11., vor 8 Uhr morgens.