Mathematik I, Logik und Algebra, WS2011/12
M. Hortmann

Blatt 8

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen								**Gruppe**	**Tutor**
1a	b	c	2a	b	c	d	e	**Summe**	**bearbeitet**
1	1	1	1	1	1	1	1	6 Punkte=100%	

Aufgabe 1

Sei G eine (multiplikativ geschriebene) Gruppe, $U \subset G$ eine Untergruppe. Man zeige:

a) Durch $x \sim y :\Leftrightarrow y^{-1}x \in U$ ist auf G eine Äquivalenzrelation definiert.
b) Ist $x \in G$ und setzt man $xU := \{ xu \mid u \in U \}$, so ist $\overline{x} = xU$. [1]
c) Man finde eine bijektive Abbildung zwischen zwei beliebigen Linksnebenklassen xU und yU und weise deren Bijektivität nach.

Aufgabe 2

Sei G eine (multiplikativ geschriebene) Gruppe und $x \in G$. Man setzt $< x > := \{ x^n \mid n \in \mathbb{Z} \}$ [2].
Aufgrund der Potenzregeln ist $< x >$ eine Untergruppe von G; man nennt sie "die von x erzeugte Untergruppe" und setzt ord(x):=|$< x >$|, d.h. "die Ordnung von x" wird definiert als Elementezahl der von x erzeugten Untergruppe; diese kann natürlich auch ∞ sein. Man nennt die Elementezahl $|G|$ der Gesamtgruppe auch "Ordnung der Gruppe G". Ist ord $(x) = n$, so ist nicht schwer zu zeigen, daß dies die kleinste natürliche Zahl ist, für die gilt: $x^n = e$. Ist $m \in \mathbb{N}$ eine weitere natürliche Zahl mit $x^m = e$, so ist ord(x) ein Teiler von m. Ist G endlich und m=|G|, so gilt $x^m = e$; also ist die Ordnung eines Elements Teiler der Gruppenordnung. Diese Tatsachen werden in der Vorlesung bewiesen.

a) Man gebe jeweils ein Beispiel (mit Beweis) für eine Gruppe G mit einem Element $x \in G$, für welches gilt: ord(x)= ∞ bzw. ord(x)=7.

---

1 Man nennt xU "Linksnebenklasse von U". Die Aussage b) bedeutet dann gerade, daß die Äquivalenzklassen der in a) definierten Äquivalenzrelation gerade Linksnebenklassen sind. Daher können wir unser Wissen über Äquivalenzklassen auf Linksnebenklassen übertragen, z.B. sind verschiedene Linksnebenklassen disjunkt.

2 Schreibt man die Gruppe additiv, so benutzt man keine Potenzschreibweise, sondern setzt stattdessen $0x := 0$, sowie für $n \in \mathbb{N}$ $nx := \underbrace{x + \ldots + x}_{n-\text{mal}}$, und schließlich $(-n)x := n(-x)$, so daß jetzt nx für alle $n \in \mathbb{Z}$ definiert ist.
Damit wird $< x > := \{ nx \mid n \in \mathbb{Z} \}$

b) Man berechne ord(2) in der Gruppe $\mathbb{Z}_n^*$ für die Fälle $n=2^{127}-1$ und $n=2^{16}+1$.

c) Ist n eine Primzahl, so ist $|\mathbb{Z}_n^*|=|\mathbb{Z}_n\setminus\{0\}|=n-1$. Für jedes $x\in\mathbb{Z}_n^*$ gilt daher: $x^{n-1}=1$ in $\mathbb{Z}_n^*$. Man zeige, daß $n=2^{32}+1$ keine Primzahl ist.

d) Man betrachte $n=2^{100}-1$ und finde ohne Benutzung eines Computers eine nicht-triviale Produktzerlegung dieser Zahl.

e) Man betrachte $n=2^{100}+1$ und finde ohne Benutzung eines Computers einen nicht-trivialen Teiler dieser Zahl.

Hinweise:

zu c) Wählen Sie in $\mathbb{Z}_n^*$ ein geeignetes x und berechnen Sie in $\mathbb{Z}_n^*$ das Element $x^{n-1}=x^{2^{32}}$ durch 32 fach wiederholtes Quadrieren und nach jedem Quadrierschritt bei Division durch n Berechnen des Rests. Dokumentieren Sie alle Rechenschritte. (Die Rechnung läßt sich auf jedem Taschenrechner durchführen, der mit Zahlen bis zu 2^{64} rechnen kann, z.B. dem im "Windows-Zubehör" .)

zu d) Die Lösung ist ganz einfach.

zu e) Ist $x\in\mathbb{Z}$, so zeigt man - z.B. durch Induktion - sehr leicht: $\forall\, n\in\mathbb{N}:\ 1-x^n=(1-x)\sum_{i=0}^{n-1}x^i$.

Ist dann $n\in\mathbb{N}$, n ungerade, so folgt sofort

$$x^n+1=1+x^n=1-(-1)^n x^n=1-(-x)^n=\left(1-(-x)\right)\sum_{i=0}^{n-1}(-x)^i=(x+1)\left(1-x+x^2\mp\ldots+x^n\right).$$

Unter Voraussetzung dieser Formel schreibt man nun einen Faktor von $2^{100}+1$ sofort hin..