Mathematik I, Logik und Algebra, WS2010/11
M. Hortmann

Blatt 10

Aufgabe 5 („Forschungsaufgabe“ :-))
Sei $n \in \mathbb{N}$.
a) Welche Ordnung hat die multiplikative Gruppe $\mathbb{Z}_{2^n}^*$? (Begründung!)
b) Man zeige, daß $\mathbb{Z}_8^*$ nicht zyklisch ist.
c) Stellen Sie an Hand von (zu dokumentierenden) Experimenten fest, welche Ordnung ein Element von $\mathbb{Z}_{2^n}^*$ höchstens haben kann.
d) Beschreiben Sie anhand von (zu dokumentierenden) Experimenten die Elemente von $\mathbb{Z}_{2^n}^*$, die die in c) festgestellte maximale Ordnung besitzen.
e) Beweisen Sie Ihr in d) gefundenes Ergebnis!

Lösung 5e:
Experimentell hat man festgestellt:

```
(13:40) gp > forstep(i=1,8,2,print1(i," ",znorder(Mod(i,8))," "))
1 1    3 2    5 2    7 2

(13:40) gp > forstep(i=1,16,2,print1(i," ",znorder(Mod(i,16))," "))
1 1    3 4    5 4    7 2    9 2    11 4    13 4    15 2

((13:40) gp > forstep(i=1,32,2,print1(i," ",znorder(Mod(i,32))," "))
 1 1    3 8    5 8    7 4    9 4    11 8    13 8    15 2
17 2   19 8    21 8   23 4    25 4    27 8    29 8    31 2
```

In $\mathbb{Z}_{16}^*$ haben also genau die Elemente 3,5,11,13 die maximale Ordnung 4,
In $\mathbb{Z}_{32}^*$ haben genau die Elemente 3,5,11,13,19,21,27,29 die maximale Ordnung 8.

Wir vermuten also den **Satz**:
0. Die Gruppen $\mathbb{Z}_2^*$ und $\mathbb{Z}_4^*$ sind zyklisch.
1. Ist $n \geq 3$, so ist die Gruppe $\mathbb{Z}_n^*$ nicht zyklisch.
2. Ist $n \geq 4$, so besitzt ein Element $x \in \mathbb{Z}_n^*$ genau dann die maximale Ordnung 2^{n-2} , wenn $x \% 8 = 3$ oder $x \% 8 = 5$.

Beweis:
ad 0: Es ist $\mathbb{Z}_2^* = \{1\}$. 1 ist Erzeuger. Es ist $\mathbb{Z}_4^* = \{1,3\} = \{1,-1\}$ 3=-1 ist Erzeuger.

ad 1: Es ist $\mathbb{Z}_8^* = \{1,3,5,7\}$. 1 besitzt die Ordnung 1; 3,5,7 besitzen die Ordnung 2. Ein Erzeuger müßte die Ordnung 4 haben. $\mathbb{Z}_8^*$ ist also nicht zyklisch.
Wir zeigen jetzt induktiv, daß $\mathbb{Z}_{2^n}^*$ für $n \geq 3$ keinen Erzeuger besitzt. Den Induktionsanfang haben wir gerade mit der Untersuchung von $\mathbb{Z}_8^*$ geleistet.

Sei ab jetzt $n>3$. Wir nehmen ein $x \in \mathbb{Z}_{2^n}^*$ und zeigen, daß x kein Erzeuger dieser 2^{n-1} -elementigen Gruppe sein kann. Fassen wir x als natürliche Zahl auf, so ist x ungerade und es gilt $1 \leq x \leq 2^n - 1$.

Jetzt kann man 2 Fälle unterscheiden:

1. Fall: $1 \leqslant x \leqslant 2^{n-1}-1$
Fassen wir *x* auf als Element von $\mathbb{Z}^*_{2^{n-1}}$, so wissen wir bereits, daß es in dieser Gruppe kein Erzeuger ist, also nicht die Ordnung 2^{n-2} besitzt. Seine Ordnung muß also ein echter Teiler von 2^{n-2} sein, also ein Teiler von 2^{n-3}. In $\mathbb{Z}^*_{2^{n-1}}$ gilt also $x^{2^{n-3}}=1$, und daher ist die natürliche Zahl $x^{2^{n-3}}-1$ durch 2^{n-1} teilbar. Nach der 3. binomischen Formel gilt: $x^{2^{n-2}}-1=(x^{2^{n-3}}-1)(x^{2^{n-3}}+1)$. Wir haben gerade gezeigt, daß der erste Faktor auf der rechten Seite durch 2^{n-1} teilbar ist und der zweite Faktor ist jedenfalls durch 2 teilbar (Potenz einer ungeraden Zahl ist ungerade). Also ist die linke Seite durch 2^n teilbar, d.h. $x^{2^{n-2}}-1=0$ in $\mathbb{Z}_{2^n}$, also $x^{2^{n-2}}=1$ in $\mathbb{Z}^*_{2^n}$. Damit hat *x* eine Ordnung, die 2^{n-2} teilt, kann also nicht Erzeuger der Gruppe $\mathbb{Z}^*_{2^n}$ sein, welche die Ordnung 2^{n-1} hat.

2. Fall: $2^{n-1}+1 \leqslant x \leqslant 2^n-1$
Wir bilden $y:=x-2^{n-1}$, und haben damit $1 \leqslant y \leqslant 2^{n-1}$. Für *y* argumentieren wir wie im 1. Fall: *y* ist kein Erzeuger von $\mathbb{Z}^*_{2^n}$, also ist $y^{2^{n-2}}-1$ durch 2^n teilbar. Wenn wir daraus folgern können, daß auch $x^{2^{n-2}}-1$ durch 2^n teilbar ist, sind wir fertig.

Es ist $x^{2^{n-2}}-1=(y+2^{n-1})^{2^{n-2}}-1$. Wir entwickeln den 1. Summanden auf der rechten Seite mit Hilfe der binomischen Formel und stellen den letzten und vorletzten Summanden der binomischen Entwicklung nach außen, also

$$\left(y^{2^{n-2}}-1\right)+2^{n-2}\,y^{2^{n-2}-1}\,2^{n-1}+\sum_{i=0}^{2^{n-2}-2}\binom{2^{n-2}}{i}y^i\left(2^{n-1}\right)^{2^{n-2}-i}.$$

Der letzte Ausdruck besteht aus drei Summanden.
Wenn wir zeigen, daß jeder von ihnen durch 2^n teilbar ist, sind wir fertig.

Der erste Summand ist $\left(y^{2^{n-2}}-1\right)$. Wir wissen bereits, daß er durch 2^n teilbar ist.

Der zweite Summand ist $2^{n-2}\,y^{2^{n-2}-1}\,2^{n-1}$. Wegen $n \geqslant 3$ ist $2^{n-2}\,2^{n-1}$ durch 2^n teilbar.

Der dritte Summand ist die Summe $\sum_{i=0}^{2^{n-2}-2}\binom{2^{n-2}}{i}y^i\left(2^{n-1}\right)^{2^{n-2}-i}$. In dieser Summe ist der Exponent $2^{n-2}-i$ immer größer als 1, also $\left(2^{n-1}\right)^{2^{n-2}-i}$ immer durch 2^n teilbar. Also ist jeder Summand und damit die Gesamtsumme durch 2^n teilbar.

Zum Beweis der letzten Teilaussage des Satzes argumentieren wir genauso rekursiv mit den bereits gewonnenen Ergebnissen Aussagen für die Gruppe $\mathbb{Z}^*_{n-1}$, beginnend mit der Aussage für $\mathbb{Z}^*_{16}$.