Die multiplikative Gruppe eines endlichen Körpers ist zyklisch

Zunächst Beispiele:

1. $\mathbb{Z}_{11}^{*}=\{1,2,3,4,5,6,7,8,9,10\}$

a	1	2	3	4	5	6	7	8	9	10
2^a	2	4	8	5	10	9	7	3	6	1

es kommen also alle Gruppenelemente als Potenzen von 2 vor: 2 ist Erzeuger von $\mathbb{Z}_{11}*$.

2. Das Polynom $f=X^2+1$ ist nicht irreduzibel in $\mathbb{Z}_2[X]$, aber in $\mathbb{Z}_3[X]$. Daher ist $F=\mathbb{Z}_3[X]/<f>$ ein Körper. Die Elemente sind Restklassen von Polynomen modulo f. In jeder Restklasse liegt genau ein Repräsentant, welcher ein Polynom höchstens ersten Grades ist. Wir beschreiben ein Polynom jetzt durch den aus seinen Koeffizienten gebildeten String, schreiben also z.B. 21 sowohl für das Polynom 2*X*+1 wie auch für seine Restklasse in *F*. Somit können wir die 9 Elemente von F so auflisten:

$F=\{0,1,2,10,11,12,20,21,22\}$.

Wegen $\overline{X^2+1}=\overline{0}$ gilt $\overline{X}^2=\overline{-1}=\overline{2}$, also läßt sich schreiben 100=2 bzw. $10\cdot 10=2$ und somit erhalten wir folgende Multiplikationstabelle bzw. Gruppentafel für *F**

		1	2	10	11	12	20	21	22
1		1	2	10	11	12	20	21	22
2		2	1	20	22	21	10	12	11
10		10	20	2	12	22	1	11	21
11		11	22	12	20	1	21	2	10
12		12	21	22	1	10	11	20	2
20		20	10	1	21	11	2	22	12
21		21	12	11	2	20	22	10	1
22		22	11	21	10	2	12	1	20

Dabei rechnet man wie in der Schule, z.B.

```
22 . 22
     11
+  11
=  121=21
        +  2
        =20
```

außer, daß es beim Addieren in den Spalten keine Überträge gibt. Auf der Basis dieser Multiplikationstabelle stellen wir fest, daß 10=*X* kein Erzeuger von *F** ist

a	1	2	3	4	5	6	7	8
10^a	10	2	20	1	10	2	20	1

denn offenbar wird von 10 nur eine Untergruppe der Ordnung 4 erzeugt. Probieren wir es dagegen mit 11=*X*+1 , so erhalten wir

a	1	2	3	4	5	6	7	8
11^a	11	20	21	2	22	10	12	1

und sehen: 11 ist ein Erzeuger der multiplikativen Gruppe von F^* , die somit zyklisch ist.

Um dies für einen beliebigen Körper K zu beweisen, benötigen wir als spezielle Körpereigenschaft nur den folgenden

Satz: Ein vom Nullpolynom verschiedenes, (oBdA normiertes) Polynom in $K[X]$ besitzt höchstens so viele Nullstellen wie sein Grad angibt.

Dies läßt sich leicht durch Induktion beweisen:
1. Ein vom Nullpolynom verschiedenes Polynom vom Grad Null ist eine von 0 verschiedene Konstante des Körpers und besitzt daher keine Nullstelle.
2. Ist $f \in K[X]$ normiert vom Grad d+1 und besitzt keine Nullstelle, so sind wir fertig. Besitzt f die Nullstelle $a \in K$, so führen wir im Euklidischen Ring $K[X]$ die Division mit Rest mit dem normierten Polynom 1sten Grades $X-a$ aus, also $f=g(X-a)+r$ mit grad $r < 1$ oder $r=0$. Setzt man a auf beiden Seiten der Gleichung ein ergibt sich, daß $r=0$, also gibt es ein Polynom g mit $f=g(X-a)$. Aus der Gradformel folgt, daß grad $g = d$. Weil nach Induktionsvoraussetzung g höchstens d Nullstellen besitzt, kann f höchstens $d+1$ Nullstellen haben.

Ist $R=\mathbb{Z}_n$, wobei n keine Primzahl ist, so ist R kein Integritätsring. Ist z.B. $n=15$, so besitzt das Polynom $X^2-1 \in R[X]$ die Nullstellen $1,4,11,14 \in R$, dies sind offenbar mehr als 2=grad f . Im Ring $R[X]$ gilt aber auch nicht die Gradformel und es gibt keine Division mit Rest wie in den Polynomringen mit Koeffizienten in einem Körper.

Satz: Die multiplikative Gruppe eines endlichen Körpers ist zyklisch

Beweis: In einer endlichen abelschen Gruppe G – z.B. der multiplikativen Gruppe eines endlichen Körpers – existiert zweifellos ein Element g von maximaler Ordnung n . Jedenfalls ist n ein Teiler der Gruppenordnung $|G|$.

Weiter unten werden wir zeigen, daß die Ordnung jedes Elements von G ein Teiler von n ist. Dies bedeutet, daß $\forall a \in G: a^n = 1$. Damit erfüllen alle Elemente von G die Gleichung $X^n - 1 = 0$.

Nehmen wir für G die multiplikative Gruppe eines endlichen Körpers, so wären demnach alle Elemente Nullstellen des Polynoms $X^n - 1$. Da dieses aber nicht mehr als n Nullstellen besitzen kann, ergibt sich die Gleichung $n = |G|$, damit wissen wir, daß ein Element maximaler Ordnung ein Erzeuger und damit die multiplikative Gruppe eines endlichen Körpers zyklisch ist. Gibt es einen Erzeuger, so gibt es viele:

Satz: In einer zyklischen Gruppe G mit n Elementen gibt es $\varphi(n)$ Erzeuger.

Beweis: Sei $g \in G$ erzeugendes Element. Definitionsgemäß ist $\varphi(n)$ die Anzahl der zu n teilerfremden natürlichen Zahlen zwischen 1 und n . Ist also $0<k<l<n$ und ggT(k, n)=1, so sind g^k und g^l verschieden, denn sonst wäre $g^{l-k} = 1$, jedoch kann keine Potenz von g mit einem Exponenten kleiner als n gleich 1 sein.

Andererseits ist g^k selbst Erzeuger der Gruppe, denn aus $1 = (g^k)^d = g^{kd}$ folgt, daß n Teiler von kd ist. Weil aber n und k teilerfremd sind, muß n Teiler von d sein, d.h. n ist Ordnung von g^k .

Ein Erzeuger der Gruppe muß natürlich die Form g^m haben mit $0<m<n$. Wären m,n nicht teilerfremd, so gäbe es einen gemeinsamen Teiler d von m und n, der größer als 1 wäre . Dann hätte man aber $(g^m)^{\frac{n}{d}}=(g^n)^{\frac{m}{d}}=1^{\frac{m}{d}}=1$, d.h. g^m hätte eine kleinere Ordnung als n und könnte somit nicht Erzeuger der gesamten Gruppe sein.

Insgesamt haben wir gezeigt: Es gibt genausoviele Erzeuger von G wie es teilerfremde Zahlen zu n zwischen 1 und n gibt.

Jetzt fehlt noch der Beweis des oben benutzten Lemmas:

Lemma: In einer endlichen abelschen Gruppe ist die Ordnung jedes Elements Teiler der Ordnung eines Elements maximaler Ordnung.

Zum Beweis benötigen wir ein weiteres
Lemma: Ist *G* eine abelsche Gruppe und sind $a,b\in G$, ord(*a*)=*m* und ord(*b*)=*n* , so besitzt das Produkt *ab* die Ordnung kgV(*m*,*n*) .

Beweis des ersten Lemmas:
Sei $b\in G$ ein Element maximaler Ordnung n und $a\in G$ ein weiteres Element mit Ordnung m. Jedenfalls ist $m\leqslant n$. Wäre $m<n$, so hätte nach dem zweiten Lemma hätte das Element ab die Ordnung kgV(m,n) . Wäre dann m kein Teiler von n, so wäre kgV(m,n)>n , d.h. das Element ab hätte eine Ordnung größer als n, was der Wahl von n als maximaler Ordnung widerspricht. Also ist m Teiler von n.

Beweis des zweiten Lemmas:
1. Fall: m, n sind teilerfremd:
$(ab)^{mn}=a^m b^n=1$.
Sei $1=(ab)^d=a^d b^d$. Dann folgt $a^d=b^{-d}$, also $a^{nd}=b^{nd}=(b^n)^d=1^d=1$. Also ist m ein Teiler von nd . Weil m und n teilerfremd sind, muß m bereits Teiler von d sein[1]. Analog erhält man, daß n Teiler von d ist, und aus der Teilerfremdheit von m,n folgt wieder, daß dann mn Teiler von d ist.

Damit ist nachgewiesen, daß mn die Ordnung von ab ist.

2. Fall: m, n sind nicht teilerfremd.
Wir benutzen die eindeutige Primfaktorzerlegung von $m=\prod_p p^{e_p}$ und $n=\prod_p p^{f_p}$. Indem wir $g_p=\max\{e_p,f_p\}$ setzen, haben wir $\mathrm{kgV}(m,n)=\prod_p p^{g_p}$. Nun sind die endlich vielen Primzahlpotenzen p^{g_p} , für die $g_p>0$ ist, paarweise teilerfremd. Wenn wir für diese Primzahlen p Gruppenelemente a_p mit der Ordnung p^{g_p} finden können, so hätte wg. Fall 1 ihr Produkt die Ordnung $\prod_p p^{g_p}=\mathrm{kgV}(m,n)$, und alles wäre bewiesen.

Sei daher p gegeben, und oBdA sei $1\leqslant f_p\leqslant e_p=g_p$.
Man zeigt nun leicht, daß $a_p:=a^{\frac{m}{p^{e_p}}}$ die Ordnung $e_p=g_p$ besitzt.

1 Dieser Schluß wurde in der Vorlesung fälschlicherweise in Zweifel gezogen.