Zum Abschluß und als Anwendung wollen wir noch die multiplikative Gruppe $(K^\star, \cdot)$ eines endlichen Körpers K untersuchen. Das Ergebnis werden wir später benötigen. Wenn K 4 oder 8 Elemente enthält, so hat $K^\star$ 3 bzw. 7 Elemente und ist daher zyklisch. Dies gilt aber auch allgemein:

(4.18) SATZ: Sei K ein Körper. Dann ist jede **endliche** Untergruppe U von $(K^\star, \cdot)$ zyklisch. Insbesondere ist die multiplikative Gruppe eines endlichen Körpers zyklisch.

Bew: Der Beweis benötigt Ergebnisse aus der Gruppentheorie, wie sie etwa im letzten Semester in der Vorlesung "Grundzüge der Algebra" bereitgestellt wurden.

$(U, \cdot)$ ist eine endliche abelsche Gruppe. Sei $n := |U|$. Die Menge $\{\mathrm{ord}(b) | b \in U\} \subseteq \mathbb{N}$ der Ordnungen aller Elemente aus U ist endlich und besitzt daher ein größtes Element m. Sei $a \in U$ mit $\underline{\mathrm{ord}(a) = m}$. Wir zeigen anschließend

$$(\star) \quad \forall\, b \in U \,:\, \mathrm{ord}(b) \,|\, m$$

Hieraus ergibt sich dann die Behauptung: Wegen $(\star)$ gibt es für ein beliebiges $b \in U$ ein $t \in \mathbb{N}$ mit $\mathrm{ord}(b) \cdot t = m$, also $b^m = (b^{\mathrm{ord}(b)})^t = 1^t = 1 \in K$, d.h.

$$(\star\,\star) \quad \forall\, b \in U \,:\, b^m = 1$$

Betrachte das Polynom $f := T^m - 1 \in K[T]$. Bezeichnet N die Menge der in K gelegenen Nullstellen von f, so gilt nach (4.7) $|N| \le \mathrm{grad}(f) = m$. Für ein beliebiges $b \in U$ folgt wegen $(\star\star)$ $f(b) = 0$, also $b \in N$. Folglich $U \subseteq N$ und $|U| \le |N| \le m = \mathrm{ord}(a) \le |U|$, woraus sich $\underline{|U| = \mathrm{ord}(a)}$ ergibt. Aus $< a > \subseteq U$ und $| < a > | = \mathrm{ord}(a) = |U|$ folgt dann aber $U = < a >$, d.h. U ist zyklisch mit a als erzeugendem Element.

Nachweis von $(\star)$: Annahme: es existiert ein Element $c \in U$ mit $\underline{\mathrm{ord}(c) \not| \; m}$. Sei $l := \mathrm{ord}(c)$. Wegen der Möglichkeit der eindeutigen Primfaktorzerlegung muß es eine Primzahl p geben, die als Faktor in l mit einer höheren Vielfachheit vorkommt als in m, d.h.

$$l = p^\lambda \cdot l' \;\text{ mit }\; \mathrm{ggT}(p, l') = 1 \quad , \quad m = p^\mu \cdot m' \;\text{ mit }\; \mathrm{ggT}(p, m') = 1 \quad , \quad \underline{\lambda > \mu}$$

Es folgt

$$\mathrm{ord}(a^{p^\mu}) = \frac{\mathrm{ord}(a)}{p^\mu} = \frac{m}{p^\mu} = \frac{p^\mu m'}{p^\mu} = m' \quad , \quad \mathrm{ord}(c^{l'}) = \frac{\mathrm{ord}(c)}{l'} = \frac{l}{l'} = \frac{p^\lambda l'}{l'} = p^\lambda$$

Sei $d := a^{p^\mu} \cdot c^{l'} \in U$. Da a^{p^μ} und $c^{l'}$ vertauschbar sind und ihre Ordnungen teilerfremd sind, ergibt sich

$$\mathrm{ord}(d) = \mathrm{ord}(a^{p^\mu} \cdot c^{l'}) = \mathrm{ord}(a^{p^\mu}) \cdot \mathrm{ord}(c^{l'}) = m' \cdot p^\lambda = m \cdot \underbrace{p^{\lambda-\mu}}_{\ge 2} > m = \mathrm{ord}(a)$$

Dies steht im **Widerspruch** dazu, daß a als ein Element größter Ordnung aus U gewählt war. Damit ist die Gültigkeit von $(\star)$ nachgewiesen. •