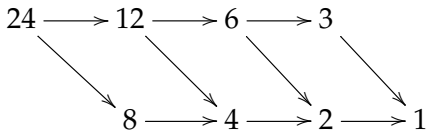
Zusatz zu Aufgabe 15

i) **Satz:**
Sei $a \in \mathbb{F}_q$ mit $a^m = 1$ und $m = \prod p_i^{n_i}$, dann:

$$\operatorname{ord}(a) = m \iff a^{m/p_i} \neq 1 \quad \forall\, i$$

Beweis: Übungsaufgabe.

ii) Sei $q = 24$ wie in Aufgabe 15. Betrachte folgendes Teilerdiagramm



iii) Aus dem Satz schließt man:
24 ist nicht die Ordnung von β, da $\beta^{24/3} = \beta^8 = 1$.
Aus $\beta^4 \neq 1$ und $\beta^8 = 1$ folgt: $\operatorname{ord}(\beta) = 8$ und insbesondere: $\beta^3 \neq 1$, $\beta^6 \neq 1$ und $\beta^{12} \neq 1$.

iv) Andere Begründung/Beweisidee:
Sei $\beta^8 = 1$. Betrachte die Untergruppen $H := \langle \beta \rangle < G := \{\beta, \ldots, \beta^8 = 1\} < \mathbb{F}_q^*$.

Die Ordnung von β kann nicht 3, 6 oder 12 sein, da nach dem Satz von Lagrange die Ordnung von H die Ordnung von G, also 8, teilen muss. Daher bleiben für $\operatorname{ord}(H) = |H| = \operatorname{ord}(\beta)$ nur die Zahlen 4 und 2 übrig. Wenn wir $\beta^4 \neq 1$ gezeigt haben, sind wir also fertig.

Ein Beweis über die Beziehung $\operatorname{ord}(\beta = \alpha^i) = \dfrac{\operatorname{ord}(\alpha)}{\operatorname{ggT}(i, \operatorname{ord}(\alpha))}$, $\operatorname{ord}(\alpha) = q - 1$ geht ähnlich.

v) **Übungsaufgabe:** Finde mit Maple in $\mathbb{F}_{401}$ je ein Element mit Ordnung 200, 100, 80, ...Welche Ordnung hat 2?