2. Untergruppen

Definition: Es sei $(G, \cdot)$ eine Gruppe. Eine Menge $H \subseteq G$, $H \neq \varnothing$ heißt Untergruppe von G, falls $(H, \cdot)$ selbst eine Gruppe ist. (D.h. H ist mit der Verknüpfung von G selbst eine Gruppe.) Wir schreiben dafür $H \leq G$.

Bemerkungen: 1) Insbesondere ist $H(\leq G)$ bezüglich der Verknüpfung von G abgeschlossen.
2) Ist G eine Gruppe, so ist $\{e\} \leq G$ und $G \leq G$. Es gibt allerdings Gruppen, die keine weiteren Untergruppen besitzen, z.B. $(\mathbb{Z}_2, +)$.
3) Ist G eine Gruppe, $H \leq G$ und $K \leq H$, so gilt auch $K \leq G$.
4) Es ist richtig, aber nicht selbstverständlich, dass das neutrale Element e_G einer Gruppe G und das neutrale Element e_H ihrer Untergruppe H übereinstimmen. Bezeichnet e_H^{-1} das inverse Element von e_H in G, so folgt aus $e_H \cdot e_H = e_H = e_H \cdot e_G$, dass

$$e_H = e_H^{-1} \cdot e_H \cdot e_H = e_H^{-1} \cdot e_H \cdot e_G = e_G.$$

Diese Tatsache folgt *nicht* aus Satz 2, da die analoge Aussage für Monoide falsch ist.
5) Ist $a \in H(\leq G)$, so stimmen die inversen Elemente von a in H und von a in G überein (was aus Satz 3 folgt).

Satz 10: Es sei G eine Gruppe und und $H \subseteq G$, $H \neq \varnothing$. Dann sind äquivalent:

(i) $H \leq G$,
(ii) $ab \in H \ \forall a, b \in H$ und $a^{-1} \in H \ \forall a \in H$,
(iii) $ab^{-1} \in H \ \forall a, b \in H$.

Beweis: (i) $\Rightarrow$ (ii) Trivial.
(ii) $\Rightarrow$ (iii) $b \in H \Rightarrow b^{-1} \in H$ und $a, b^{-1} \in H \Rightarrow ab^{-1} \in H$.
(iii) $\Rightarrow$ (i) $H \neq \varnothing \Rightarrow \exists x \in H$. Daher $e = xx^{-1} \in H$ und $a^{-1} = ea^{-1} \in H \ \forall a \in H$ sowie $ab = a(b^{-1})^{-1} \in H \ \forall a, b \in H$. Da Assoziativität auf ganz G gilt, gilt sie auch auf H und $(H, \cdot)$ ist eine Gruppe.

Bemerkungen: 1) Wird die Gruppe $(G, +)$ additiv geschrieben, so wird Bedingung (ii) zu $a + b \in H \ \forall a, b \in H$ und $-a \in H \ \forall a \in H$ und (iii) zu $a - b \in H \ \forall a, b \in H$.
2) Um $H \leq G$ zu zeigen, überprüft man üblicherweise Bedingung (ii) oder (iii) aus Satz 10.
3) Der einfachste Weg, zu zeigen, dass es sich bei $(G, \cdot)$ um eine Gruppe handelt, ist oft, zu zeigen, dass G Untergruppe einer bekannten Gruppe ist.

Beispiele: 1) Ist V ein Vektorraum und W ein Teilraum von V, so ist $(W, +)$ Untergruppe von $(V, +)$.
2) $(\mathbb{Z}, +)$ ist Untergruppe von $(\mathbb{Q}, +)$, $(\mathbb{Q}, +)$ von $(\mathbb{R}, +)$ und $(\mathbb{R}, +)$ von $(\mathbb{C}, +)$.

3) $\big(\{+1,-1\},\cdot\big)$ ist Untergruppe von $\big(\mathbb{Q}\setminus\{0\},\cdot\big)$, $\big(\mathbb{Q}\setminus\{0\},\cdot\big)$ von $\big(\mathbb{R}\setminus\{0\},\cdot\big)$ und $\big(\mathbb{R}\setminus\{0\},\cdot\big)$ von $\big(\mathbb{C}\setminus\{0\},\cdot\big)$.
4) Für jedes $m\in\mathbb{Z}$ ist $(m\mathbb{Z},+)$ Untergruppe von $(\mathbb{Z},+)$ (wobei $m\mathbb{Z}=\{mk\mid k\in\mathbb{Z}\}$).
5) Ist K ein Körper, so ist $\mathrm{SL}_n(K)$ Untergruppe von $\mathrm{GL}_n(K)$.
6) Es sei K ein Körper und

$$T:=\big\{\mathrm{diag}(a_1,\dots,a_n)\mid a_1,\dots,a_n\in K\setminus\{0\}\big\}$$

(wobei $\mathrm{diag}(a_1,\dots,a_n)$ die Diagonalmatrix mit den Eintragungen $a_1,\dots,a_n$ bezeichnen soll). Dann ist T Untergruppe von $\mathrm{GL}_n(K)$, da

$$\det\big(\mathrm{diag}(a_1,\dots,a_n)\big)=a_1\cdots a_n\neq 0$$

und daher $T\subseteq\mathrm{GL}_n(K)$ und

$$\begin{aligned}\mathrm{diag}(a_1,\dots,a_n)\cdot\mathrm{diag}(b_1,\dots,b_n)^{-1}&=\mathrm{diag}(a_1,\dots,a_n)\cdot\mathrm{diag}\big(b_1^{-1},\dots,b_n^{-1}\big)\\&=\mathrm{diag}\big(a_1b_1^{-1},\dots,a_nb_n^{-1}\big)\in T\end{aligned}$$

für $a_1,\dots,a_n,b_1,\dots,b_n\in K\setminus\{0\}$ beliebig.
7) Ist $m\in\mathbb{N}\setminus\{0,1\}$ und bezeichnet

$$\big(\mathbb{Z}_m^*\big)^2=\big\{\overline{a}^2\,\big|\,\overline{a}\in\mathbb{Z}_m^*\big\}$$

die Menge der quadratischen Reste modulo m (siehe Zahlentheorie), so ist $\big(\mathbb{Z}_m^*\big)^2$ eine Untergruppe von $\mathbb{Z}_m^*$, da

$$\overline{a}^2\Big(\overline{b}^2\Big)^{-1}=\Big(\overline{a}\overline{b}^{-1}\Big)^2\in\big(\mathbb{Z}_m^*\big)^2$$

für alle $\overline{a},\overline{b}\in\mathbb{Z}_m^*$.
8) Bezeichnet $\{I,R,S_1,S_2\}$ die oben beschriebene Symmetriegruppe des Rechtecks, so sind $\{I,R\}$, $\{I,S_1\}$ und $\{I,S_2\}$ Untergruppen von $\{I,R,S_1,S_2\}$.

Lemma 11: Es sei G eine Gruppe.
(i) Ist $I\neq\varnothing$ eine (Index)Menge und $H_i\leq G\ \forall i\in I$, so ist $\bigcap\limits_{i\in I}H_i\leq G$.
(ii) Wenn $H_1\leq G$ und $H_2\leq G$, so gilt $H_1\cup H_2\leq G\Leftrightarrow H_1\subseteq H_2$ oder $H_2\subseteq H_1$.

Beweis: (i) $a,b\in\bigcap\limits_{i\in I}H_i\Rightarrow a,b\in H_i\ \forall i\in I\Rightarrow ab^{-1}\in H_i\ \forall i\in I\Rightarrow ab^{-1}\in\bigcap\limits_{i\in I}H_i$. Die Behauptung folgt nun aus Satz 10.
(ii) ($\Rightarrow$) Wäre $H_1\not\subseteq H_2$ und $H_2\not\subseteq H_1$, so $\exists a\in H_1\setminus H_2$ und $\exists b\in H_2\setminus H_1$. Nun gilt $a,b\in H_1\cup H_2\Rightarrow ab\in H_1\cup H_2\Rightarrow ab\in H_1$ oder $ab\in H_2$. Falls $ab\in H_1$, so $b=a^{-1}(ab)\in H_1$, Widerspruch. Falls $ab\in H_2$, so $a=(ab)b^{-1}\in H_2$, Widerspruch.
($\Leftarrow$) Das folgt aus $H_1\cup H_2=H_1$ oder $H_1\cup H_2=H_2$.

Definition: Es sei G eine Gruppe und $M \subseteq G$. Dann heißt

$$\langle M \rangle = \bigcap_{M \subseteq H, H \leq G} H$$

die von M erzeugte Untergruppe von G. (Wegen Lemma 11 (i) handelt es sich tatsächlich um eine Untergruppe.)
Gilt $\langle M \rangle = G$, so sagt man, G werde von M erzeugt und nennt M ein Erzeugendensystem von G.
Ist M endlich, d.h. $\exists a_1, \dots, a_n \in G : M = \{a_1, \dots, a_n\}$, so schreibt man auch $\langle a_1, \dots, a_n \rangle$ statt $\langle M \rangle$.
Wenn $\exists a_1, \dots, a_n \in G : G = \langle a_1, \dots, a_n \rangle$, so sagt man, G sei endlich erzeugt.

Bemerkungen: 1) Nach Definition gilt stets $M \subseteq \langle M \rangle$ und $\langle M \rangle$ ist die kleinste Untergruppe von G, die M enthält.
2) Ebenso gilt nach Definition für eine Untergruppe $H \leq G$ mit $M \subseteq H$, dass $\langle M \rangle \subseteq H$.
3) Weiters folgt aus der Definition $\langle \varnothing \rangle = \{e\}$ und für jede Gruppe G gilt $\langle G \rangle = G$.
4) Allgemeiner gilt für jede Untergruppe $H \leq G$, dass $\langle H \rangle = H$.
5) Ist G eine endliche Gruppe, so ist G trivialerweise endlich erzeugt, da $\langle G \rangle = G$.

Satz 12: Es sei G eine Gruppe und $M \subseteq G$, $M \neq \varnothing$. Dann ist

$$\langle M \rangle = \left\{ a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} \mid n \geq 1, a_1, \dots, a_n \in M, \varepsilon_1, \dots, \varepsilon_n \in \{1, -1\} \right\}.$$

Beweis: Es sei

$$\overline{H} = \left\{ a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} \mid n \geq 1, a_1, \dots, a_n \in M, \varepsilon_1, \dots, \varepsilon_n \in \{1, -1\} \right\}.$$

Offenbar gilt $M \subseteq \overline{H}$ und $\overline{H} \leq G$, da

$$(a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n})(b_1^{\tau_1} \dots b_m^{\tau_m})^{-1} = a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} b_m^{-\tau_m} \dots b_1^{-\tau_1} \in \overline{H}$$

für $a_1, \dots, a_n, b_1, \dots, b_m \in M$ und $\varepsilon_1, \dots, \varepsilon_n, \tau_1, \dots, \tau_m \in \{1, -1\}$. Daher ist $\langle M \rangle \subseteq \overline{H}$.
Ist $H \leq G$ und $M \subseteq H$, so muss

$$a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} \in H \ \forall a_1, \dots, a_n \in M, \ \forall \varepsilon_1, \dots, \varepsilon_n \in \{1, -1\}$$

gelten. Daraus folgt $\overline{H} \subseteq H$ und (da $H \leq G$ beliebig war) $\overline{H} \subseteq \langle M \rangle$.

Korollar 13: Ist G eine Gruppe und $a \in G$, so gilt $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$.

Beweis: Das folgt sofort aus Satz 12 wegen

$$\begin{aligned} \langle a \rangle &= \left\{ a^{\varepsilon_1} \dots a^{\varepsilon_n} \mid n \geq 1, \varepsilon_1, \dots, \varepsilon_n \in \{1, -1\} \right\} \\ &= \left\{ a^{\varepsilon_1 + \dots + \varepsilon_n} \mid n \geq 1, \varepsilon_1, \dots, \varepsilon_n \in \{1, -1\} \right\} = \{a^k \mid k \in \mathbb{Z}\}. \end{aligned}$$

Beispiele: 1) Betrachte $(\mathbb{Z},+)$. Für $m\in\mathbb{Z}$ ist $\langle m\rangle=\{km\mid k\in\mathbb{Z}\}=m\mathbb{Z}$. Insbesondere ist $\langle 1\rangle=\langle -1\rangle=\mathbb{Z}$.
2) Es sei $m\in\mathbb{N}\setminus\{0,1\}$. Betrachte $(\mathbb{Z}_m,+)$. Dann ist $\langle\overline{1}\rangle=\mathbb{Z}_m$ (da $\overline{0}=m\cdot\overline{1}$ und $\overline{k}=k\cdot\overline{1}$ für $1\leq k\leq m-1$).
3) Betrachte $(\mathbb{Z}_6,+)$. Dann ist $\mathbb{Z}_6=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\}=\langle\overline{2},\overline{3}\rangle$, da $\overline{0}=2\cdot\overline{3}$, $\overline{1}=2\cdot\overline{2}+\overline{3}$, $\overline{4}=2\cdot\overline{2}$ und $\overline{5}=\overline{2}+\overline{3}$.
4) Betrachte $(\mathbb{C}\setminus\{0\},\cdot)$. Dann ist $\langle i\rangle=\{1,i,-1,-i\}$, d.h. die vierten Einheitswurzeln.
5) Allgemeiner gilt in $(\mathbb{C}\setminus\{0\},\cdot)$: Ist $m\in\mathbb{N}\setminus\{0,1\}$, so ist $\langle e^{2\pi i/m}\rangle$ die Gruppe der m-ten Einheitswurzeln.
6) Betrachte $\mathbb{Z}_9^*=\{\overline{1},\overline{2},\overline{4},\overline{5},\overline{7},\overline{8}\}$. Hier gelten $\langle\overline{1}\rangle=\{\overline{1}\}$, $\langle\overline{2}\rangle=\mathbb{Z}_9^*$, $\langle\overline{4}\rangle=\{\overline{1},\overline{4},\overline{7}\}$, $\langle\overline{5}\rangle=\mathbb{Z}_9^*$, $\langle\overline{7}\rangle=\{\overline{1},\overline{4},\overline{7}\}$ und $\langle\overline{8}\rangle=\{\overline{1},\overline{8}\}$. (In der Zahlentheorie sagt man, 2 und 5 seien Primitivwurzeln modulo 9.)
7) Betrachte $\mathbb{Z}_8^*=\{\overline{1},\overline{3},\overline{5},\overline{7}\}$. Hier ist $\mathbb{Z}_8^*=\langle\overline{5},\overline{7}\rangle=\langle\overline{5},\overline{-1}\rangle$, da $\overline{1}=\overline{5}\cdot\overline{5}=\overline{-1}\cdot\overline{-1}$ und $\overline{3}=\overline{5}\cdot\overline{7}$.
8) Betrachte $\mathbb{Z}_{16}^*=\{\overline{1},\overline{3},\overline{5},\overline{7},\overline{9},\overline{11},\overline{13},\overline{15}\}$. Hier ist $\mathbb{Z}_{16}^*=\langle\overline{5},\overline{15}\rangle=\langle\overline{5},\overline{-1}\rangle$, da $\overline{1}=\overline{-1}^2$, $\overline{3}=\overline{5}^3\cdot\overline{-1}$, $\overline{7}=\overline{5}^2\cdot\overline{-1}$, $\overline{9}=\overline{5}^2$, $\overline{11}=\overline{5}\cdot\overline{-1}$ und $\overline{13}=\overline{5}^3$.
9) Betrachte $(\mathbb{R}^2,+)$. Dann ist

$$\left\langle\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right\rangle=\left\{k\begin{pmatrix}1\\0\end{pmatrix}+\ell\begin{pmatrix}0\\1\end{pmatrix}\;\middle|\;k,\ell\in\mathbb{Z}\right\}=\left\{\begin{pmatrix}k\\\ell\end{pmatrix}\;\middle|\;k,\ell\in\mathbb{Z}\right\}=\mathbb{Z}^2,$$

d.h. ein Gitter im $\mathbb{R}^2$.
10) Allgemeiner gilt (in $(\mathbb{R}^2,+)$): Sind $v,w\in\mathbb{R}^2$ linear unabhängig über $\mathbb{R}$, so ist $\langle v,w\rangle$ ein Gitter im $\mathbb{R}^2$.

Definition: 1) Ist G eine Gruppe, so wird die Mächtigkeit $|G|$ die Ordnung von G genannt.
2) Ist G eine Gruppe und $a\in G$, so definiert man die Ordnung $\operatorname{ord}(a)$ von a als die Ordnung von $\langle a\rangle$, d.h. $\operatorname{ord}(a)=|\langle a\rangle|$.

Bemerkung: Ist G eine Gruppe mit neutralem Element e, so gilt $\operatorname{ord}(e)=1$ und e ist das einzige Element von G mit Ordnung 1. (Wenn $a\in G$ mit $\operatorname{ord}(a)=1$, so muss wegen Korollar 13 $a^2=a$ gelten. Die Behauptung folgt nun aus Übungsbeispiel 10a).)

Beispiele: 1) Jedes $k\in\mathbb{Z}\setminus\{0\}$ hat unendliche Ordnung in $(\mathbb{Z},+)$.
2) Ebenso hat jedes $x\in\mathbb{R}\setminus\{0\}$ unendliche Ordnung in $(\mathbb{R},+)$ und jedes $z\in\mathbb{C}\setminus\{0\}$ unendliche Ordnung in $(\mathbb{C},+)$.
3) Betrachte $(\mathbb{Z}_6,+)$. Hier ist $\operatorname{ord}(\overline{1})=\operatorname{ord}(\overline{5})=6$ (da $\langle\overline{1}\rangle=\mathbb{Z}_6$ und $\langle\overline{5}\rangle=\langle\overline{-1}\rangle=\mathbb{Z}_6$), $\operatorname{ord}(\overline{2})=\operatorname{ord}(\overline{4})=3$ (da $\langle 2\rangle=\langle 3\rangle=\{\overline{0},\overline{2},\overline{4}\}$) und $\operatorname{ord}(\overline{3})=2$ (da $\langle\overline{3}\rangle=\{\overline{0},\overline{3}\}$).

4) Betrachte $(\mathbb{Z}_9^*, \cdot)$. Hier ist $\operatorname{ord}(\overline{2}) = \operatorname{ord}(\overline{5}) = 6$ (da $\langle\overline{2}\rangle = \langle\overline{5}\rangle = \mathbb{Z}_9^*$), $\operatorname{ord}(\overline{4}) = \operatorname{ord}(\overline{7}) = 3$ (da $\langle\overline{4}\rangle = \langle\overline{7}\rangle = \{\overline{1}, \overline{4}, \overline{7}\}$) und $\operatorname{ord}(\overline{8}) = 2$ (da $\langle\overline{8}\rangle = \{\overline{1}, \overline{8}\}$).
5) Betrachte $(\mathbb{C} \setminus \{0\}, \cdot)$. Hier ist $\operatorname{ord}(i) = 4$ (da $\langle i\rangle = \{1, i, -1, -i\}$) und $\operatorname{ord}(e^{2\pi i/m}) = m$, da $\langle e^{2\pi i/m}\rangle$ die Menge der m-ten Einheitswurzeln ist.

Satz 14: Es sei G eine Gruppe und $a \in G$. Dann sind äquivalent:

(i) a hat unendliche Ordnung,
(ii) $a^n = e \Leftrightarrow n = 0$ (für $n \in \mathbb{Z}$),
(iii) $a^k = a^\ell \Leftrightarrow k = \ell$ (für $k, \ell \in \mathbb{Z}$).

Beweis: (i) $\Rightarrow$ (ii) ($\Rightarrow$) Angenommen, $\exists n \in \mathbb{Z} \setminus \{0\} : a^n = e$. Da dann auch $a^{|n|} = e$, kann man o.B.d.A. $n > 0$ voraussetzen. Für $k \in \mathbb{Z}$ sei $k = qn + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < n$. Dann folgt $a^k = (a^n)^q a^r = a^r$ und daher $\langle a\rangle = \{a^k \mid k \in \mathbb{Z}\} = \{a^r \mid r \in \mathbb{Z}, 0 \leq r < n\}$, ein Widerspruch zur unendlichen Ordnung von a.
($\Leftarrow$) Diese Implikation gilt immer.
(ii) $\Rightarrow$ (iii) $a^k = a^\ell \Leftrightarrow a^{k-\ell} = e \overset{\text{(ii)}}{\Leftrightarrow} k - \ell = 0 \Leftrightarrow k = \ell$
(iii) $\Rightarrow$ (i) Nach Voraussetzung ist $a^k \neq a^\ell$ für $k, \ell \in \mathbb{Z}$, $k \neq \ell$. Daher enthält die Untergruppe $\langle a\rangle = \{a^k \mid k \in \mathbb{Z}\}$ nur paarweise verschiedene Elemente und ist daher eine unendliche Menge.

Satz 15: Es sei G eine Gruppe und $a \in G$ habe endliche Ordnung m. Dann gelten:

(i) $m = \min\{n \in \mathbb{Z} \mid n > 0, a^n = e\}$
(ii) $\langle a\rangle = \{e, a, a^2, \ldots, a^{m-1}\} = \{a^i \mid 0 \leq i < m\}$
(iii) $a^n = e \Leftrightarrow m \mid n$ (für $n \in \mathbb{Z}$)
(iv) $a^k = a^\ell \Leftrightarrow k \equiv \ell \pmod{m}$ (für $k, \ell \in \mathbb{Z}$)
(v) Für $k \in \mathbb{Z}$ ist

$$\operatorname{ord}(a^k) = \frac{m}{\operatorname{ggT}(m, k)}.$$

Für $k \in \mathbb{Z} \setminus \{0\}$ ist

$$\operatorname{ord}(a^k) = \frac{\operatorname{kgV}(m, k)}{|k|}.$$

Insbesondere gilt: Wenn $k \mid m$ dann gilt $\operatorname{ord}(a^k) = \frac{m}{|k|}$.

Beweis: (i) und (ii) Nach Satz 14 (ii) $\exists n \in \mathbb{Z} \setminus \{0\} : a^n = e$ und wegen $a^{|n|} = e$ kann man wieder $n > 0$ voraussetzen. Sei t das kleinste derartige $n > 0$, d.h.

$$t = \min\{n \in \mathbb{Z} \mid n > 0, a^n = e\}.$$

Genau wie im Beweis von Satz 14 (i) folgt $\langle a\rangle = \{a^i \mid 0 \leq i < t\}$. Wäre $a^i = a^j$ für $0 \leq i < j < t$, so wäre $a^{j-i} = e$ mit $0 < j - i < t$, ein Widerspruch zur Minimalität von t.

Also gilt $m = |\langle a\rangle| = t$ und daher $\langle a\rangle = \{a^i \mid 0 \le i < m\}$.
(iii) ($\Rightarrow$) Es sei $n = qm + r$ mit $q, r \in \mathbb{Z}$ und $0 \le r < m$. Dann gilt $e = a^n = (a^m)^q a^r = a^r$. Da $r < m$ muss $r = 0$ gelten, d.h. $m \mid n$.
($\Leftarrow$) $a^n = (a^m)^{n/m} = e^{n/m} = e$.
(iv) $a^k = a^\ell \Leftrightarrow a^{k-\ell} = e \overset{\text{(iii)}}{\Leftrightarrow} m \mid (k-\ell) \Leftrightarrow k \equiv \ell \pmod m$.
(v) Es sei $s = \operatorname{ord}(a^k)$. Wegen $a^{ks} = (a^k)^s = e$ und (iii) folgt $m \mid (ks)$. Mithilfe eines Resultats aus der Zahlentheorie erhält man daraus

$$\frac{m}{\operatorname{ggT}(m,k)} \,\Big|\, \frac{k}{\operatorname{ggT}(m,k)} s \qquad \text{und} \qquad \frac{m}{\operatorname{ggT}(m,k)} \,\Big|\, s.$$

Andererseits ist

$$\big(a^k\big)^{m/\operatorname{ggT}(m,k)} = \big(a^m\big)^{k/\operatorname{ggT}(m,k)} = e^{k/\operatorname{ggT}(m,k)} = e,$$

woraus wegen (iii)

$$s \,\Big|\, \frac{m}{\operatorname{ggT}(m,k)}$$

folgt. Damit ist $\operatorname{ord}(a^k) = s = m/\operatorname{ggT}(m,k)$ bewiesen. Die zweite Formel für $\operatorname{ord}(a^k)$ folgt aus $\operatorname{ggT}(m,k) \cdot \operatorname{kgV}(m,k) = m|k|$ (für $k \neq 0$). Der Zusatz ergibt sich aus jeder der beiden Formeln weil $\operatorname{ggT}(m,k) = |k|$ bzw. $\operatorname{kgV}(m,k) = m$ wenn $k \mid m$.

Beispiel: Betrachte $\mathbb{Z}_9^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$. Weiß man, dass $\operatorname{ord}(\overline{2}) = 6$ ist, so kann Satz 15 (v) verwendet werden, um die Ordnung der anderen Elemente zu berechnen:

$$\operatorname{ord}\big(\overline{4}\big) = \operatorname{ord}\big(\overline{2}^2\big) = \frac{6}{\operatorname{ggT}(6,2)} = \frac{6}{2} = 3,$$

$$\operatorname{ord}\big(\overline{5}\big) = \operatorname{ord}\big(\overline{2}^5\big) = \frac{6}{\operatorname{ggT}(6,5)} = \frac{6}{1} = 6,$$

$$\operatorname{ord}\big(\overline{7}\big) = \operatorname{ord}\big(\overline{2}^4\big) = \frac{6}{\operatorname{ggT}(6,4)} = \frac{6}{2} = 3$$

und

$$\operatorname{ord}\big(\overline{8}\big) = \operatorname{ord}\big(\overline{2}^3\big) = \frac{6}{\operatorname{ggT}(6,3)} = \frac{6}{3} = 2.$$