(2) Man schreibe eine MuPAD-Funktion, die für eine natürliche Zahl $m > 1$ mit Hilfe der in (1) geschilderten Methode eine nichttriviale Faktorisierung von m findet, bzw. feststellt, daß m eine Primzahl ist.

Aufgabe 10: (1) Man vervollständige die in (2.21) gegebene Definition der MuPAD-Funktion `pollard`: Einerseits fehlen die Abfragen, die überprüfen, ob bei einem Aufruf der Funktion die übergebenen Parameter vom richtigen Typ sind, andererseits fehlt am Anfang von `pollard` die Abfrage, ob die zu faktorisierende Zahl m eine Primzahl ist; ist m eine Primzahl, so wird man das Verfahren sofort abbrechen.

(2) Man experimentiere mit der Funktion `pollard`; insbesondere ändere man die darin verwendete Funktion f ab. (Funktionen wie die in (2.21)(2) angegebenen programmiert man in MuPAD übrigens mit Hilfe der Funktion `powermod`, vgl. dazu (4.24)). Man ändere die Definition von `pollard` so ab, daß neben einem gefundenem Teiler auch die Anzahl der zum Auffinden dieses Teilers benötigten Iterationen ausgegeben wird.

Aufgabe 11: Es sei $m \in \mathbb{N}$, es sei $f : \{0, 1, \ldots, m-1\} \to \{0, 1, \ldots, m-1\}$ eine Abbildung, und es sei $x_0 \in \{0, 1, \ldots, m-1\}$. Die Folge $(x_i)_{i \geq 0}$ mit $x_i := f(x_{i-1})$ für jedes $i \in \mathbb{N}$ ist nach einer Vorperiode periodisch; es seien k die Länge der Vorperiode und l die minimale Periodenlänge. Man beweise: Für $i := l \cdot (1 + \lfloor k/l \rfloor)$ ist $x_i = x_{2i}$.

Aufgabe 12: Man schreibe eine MuPAD-Funktion zum Test von Pepin aus Abschnitt (2.22) und wende sie auf einige Fermat-Zahlen an. Man versuche, mittels der in (2.21) beschriebenen rho-Methode von Pollard (und auch mit Hilfe der MuPAD-Funktion `ifactor`) nichttriviale Faktoren einiger Fermat-Zahlen $F(n)$ mit $n \geq 5$ zu finden (vgl. Riesel [90], Tabelle 4).

Aufgabe 13: Eine natürliche Zahl n heißt teilerreich, wenn gilt: Für jede natürliche Zahl $k < n$ ist $\tau(k) < \tau(n)$. Man ermittle mittels MuPAD die ersten teilerreichen natürliche Zahlen, sehe sich ihre Primzerlegungen an, formuliere eine Vermutung und beweise sie oder lese dazu Kapitel 14 in Honsberger [46]. Mit teilerreichen Zahlen hat sich wohl zuerst der indische Zahlentheoretiker S. Ramanujan in [87] befaßt. In dieser Arbeit findet sich eine Tabelle von teilerreichen Zahlen; die größte darin ist 674 63283 88800.

3 Endliche abelsche Gruppen

(3.1) In diesem Paragraphen werden Gruppen G betrachtet, deren Verknüpfung als "Multiplikation" $(a, b) \mapsto ab : G \times G \to G$ geschrieben ist. Ist G eine solche Gruppe, so wird ihr neutrales Element mit e_G bezeichnet, und für jedes $a \in G$ wird das zu a inverse Element mit a^{-1} bezeichnet.

(3.2) Bemerkung: Es sei G eine Gruppe.
(1) Es sei $a \in G$. Man definiert für jedes $k \in \mathbb{Z}$ ein Element $a^k \in G$, und zwar so: Man setzt $a^0 := e_G$ und $a^k := a^{k-1}a$ für jedes $k \in \mathbb{N}$ und $a^k := (a^{-1})^{-k}$ für jedes $k \in \mathbb{Z}$ mit $k < 0$. (Für $k = -1$ ergibt sich dabei das zu a inverse Element der Gruppe G).
(2) Für jedes $a \in G$ und alle $j, k \in \mathbb{Z}$ gilt

$$a^j a^k = a^{j+k} = a^{k+j} = a^k a^j \quad \text{und} \quad (a^j)^k = a^{jk} = a^{kj} = (a^k)^j.$$

(3) Sind $a, b \in G$ und gilt $ab = ba$, so gilt $(ab)^k = a^k b^k$ für jedes $k \in \mathbb{Z}$.

(3.3) Bemerkung: Es sei G eine Gruppe, und es sei $a \in G$. Dann ist

$$\langle a \rangle := \{a^j \mid j \in \mathbb{Z}\}$$

eine abelsche Untergruppe von G (vgl. (3.2)(2)). $\langle a \rangle$ ist die kleinste Untergruppe von G, die a enthält, und heißt die von a erzeugte Untergruppe von G.

(3.4) Definition: Es sei G eine endliche Gruppe. Die Anzahl $\#(G)$ der Elemente von G heißt die Ordnung der Gruppe G, und für jedes $a \in G$ heißt $\operatorname{ord}(a) := \#(\langle a \rangle)$ die Ordnung des Elements a.

(3.5) Satz: *Es sei G eine endliche Gruppe, und es sei $a \in G$.*
(1) *Es gilt*

$$\operatorname{ord}(a) = \min(\{i \in \mathbb{N} \mid a^i = e_G\}) \quad \text{und} \quad \langle a \rangle = \{e_G, a, a^2, \ldots, a^{\operatorname{ord}(a)-1}\}.$$

(2) *Für ganze Zahlen j und k gilt $a^j = a^k$, genau wenn $k - j$ durch $\operatorname{ord}(a)$ teilbar ist.*
(3) *Für eine ganze Zahl j gilt $a^j = e_G$, genau wenn j durch $\operatorname{ord}(a)$ teilbar ist.*

Beweis: (a) Weil G endlich ist, existieren $j, k \in \mathbb{Z}$ mit $a^j = a^k$ und mit $j < k$, und damit gilt $i := k - j \in \mathbb{N}$ und $a^i = a^{k-j} = a^k (a^j)^{-1} = e_G$.
(b) $U := \{i \in \mathbb{Z} \mid a^i = e_G\}$ ist eine Untergruppe der Gruppe $(\mathbb{Z}, +)$, denn wegen $0 \in U$ ist $U \neq \varnothing$, und für alle $i, j \in U$ gilt $a^{i+j} = a^i a^j = e_G$ und $a^{-i} = (a^i)^{-1} = e_G$, also $i + j \in U$ und $-i \in U$. Nach (a) ist $U \neq \{0\}$, und daher gilt nach (1.6) für $m := \min(U \cap \mathbb{N})$: Es ist

$$U = m\mathbb{Z} = \{i \in \mathbb{Z} \mid m \text{ teilt } i\}.$$

(c) Für jedes $x \in \langle a \rangle$ gilt: Es gibt ein $k \in \mathbb{Z}$ mit $x = a^k$, dazu existieren ganze Zahlen q und r mit $k = mq + r$ und mit $0 \leq r \leq m - 1$, und es ist

$$x = a^k = a^{mq+r} = (a^m)^q a^r = (e_G)^q a^r = a^r \in \{e_G, a, a^2, \ldots, a^{m-1}\}.$$

Also gilt

$$\langle a \rangle = \{e_G, a, a^2, \ldots, a^{m-1}\}.$$

(d) Es seien $j, k \in \mathbb{Z}$. Wegen $a^{k-j} = a^k (a^j)^{-1}$ gilt: Es ist $a^j = a^k$, genau wenn $a^{k-j} = e_G$ ist, also genau wenn $k - j \in U$ ist, also genau wenn $k - j$ durch m teilbar ist.
(e) Sind $j, k \in \{0, 1, \ldots, m-1\}$ und gilt $a^j = a^k$, so ist $k - j$ nach (d) durch m teilbar, und wegen $-(m-1) \leq k - j \leq m - 1$ folgt $j = k$. Also sind die Elemente $e_G = a^0$, $a = a^1$, $a^2, \ldots, a^{m-1}$ von $\langle a \rangle$ paarweise verschieden. Es folgt

$$\operatorname{ord}(a) = \#(\langle a \rangle) = m = \min(U \cap N) = \min(\{i \in \mathbb{N} \mid a^i = e_G\}).$$

Damit ist der Satz bewiesen.

(3.6) Satz (J. L. Lagrange, 1736 – 1813): *Es sei G eine endliche Gruppe.*
(1) *Für jede Untergruppe U von G gilt: $\#(U)$ teilt $\#(G)$.*
(2) *Für jedes $a \in G$ gilt: Es ist $a^{\#(G)} = e_G$, und $\operatorname{ord}(a)$ teilt $\#(G)$, und zwar ist*

$$\operatorname{ord}(a) = \min(\{d \in \mathbb{N} \mid d \text{ teilt } \#(G);\ a^d = e_G\}).$$

Beweis: (1) Es sei U eine Untergruppe von G.
(a) Für $a, b \in G$ wird $a \sim b$ gesetzt, genau wenn $a^{-1}b \in U$ ist. Die so erklärte Relation $\sim$ ist eine Äquivalenzrelation auf G.
Beweis: Für jedes $a \in G$ gilt $a^{-1}a = e_G \in U$, also $a \sim a$. – Sind $a, b \in G$ und gilt $a \sim b$, so gilt $a^{-1}b \in U$ und daher auch $b^{-1}a = (a^{-1}b)^{-1} \in U$, also $b \sim a$. – Sind $a, b, c \in G$ und gilt $a \sim b$ und $b \sim c$, so gilt $a^{-1}b \in U$ und $b^{-1}c \in U$ und daher auch $a^{-1}c = (a^{-1}b)(b^{-1}c) \in U$, also $a \sim c$.
(b) Es sei $a \in G$. Dann ist $aU := \{b \in G \mid a \sim b\} = \{ax \mid x \in U\}$ die Äquivalenzklasse von a bezüglich $\sim$, und die Abbildung $x \mapsto ax : U \to aU$ ist bijektiv (mit der Umkehrabbildung $y \mapsto a^{-1}y : aU \to U$). Also gilt $\#(aU) = \#(U)$.
(c) Es seien $a_1, a_2, \ldots, a_d \in G$ mit: $a_1U, a_2U, \ldots, a_dU$ sind die verschiedenen Äquivalenzklassen bezüglich $\sim$ in G. Dann sind $a_1U, a_2U, \ldots, a_dU$ paarweise disjunkte Teilmengen von G, deren Vereinigung ganz G ist, und daher gilt

$$\#(G) = \sum_{i=1}^{d} \#(a_iU) \overset{\text{(b)}}{=} d \cdot \#(U).$$

(2) Es sei $a \in G$. Nach (1) ist $\#(G)$ durch $\#(\langle a \rangle) = \operatorname{ord}(a)$ teilbar, wegen (3.5)(3) ist daher $a^{\#(G)} = e_G$, und wegen (3.5)(1) gilt, daß $\operatorname{ord}(a)$ der kleinste Teiler $d \in \mathbb{N}$ von $\#(G)$ mit $a^d = e_G$ ist.

(3.7) Satz: *Es sei G eine endliche abelsche Gruppe.*
(1) *Es seien $a, b \in G$, und es gelte* $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$. *Dann gilt*

$$\mathrm{ord}(ab) \;=\; \mathrm{ord}(a)\,\mathrm{ord}(b).$$

(2) *Es sei $a \in G$, und es sei $k \in \mathbb{Z}$. Dann gilt*

$$\mathrm{ord}(a^k) \;=\; \frac{\mathrm{ord}(a)}{\mathrm{ggT}\big(k, \mathrm{ord}(a)\big)}.$$

Beweis: (1) Es seien $r := \mathrm{ord}(a)$, $s := \mathrm{ord}(b)$ und $t := \mathrm{ord}(ab)$. Wegen $(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r = e_G$ ist rs durch $\mathrm{ord}(ab) = t$ teilbar (vgl. (3.5)(3)). Wegen $a^{st} = a^{st}(b^s)^t = (ab)^{st} = e_G$ ist st durch $\mathrm{ord}(a) = r$ teilbar, und wegen $\mathrm{ggT}(r,s) = 1$ folgt $r \mid t$ (vgl. (1.14)(3)). Wegen $b^{rt} = (a^r)^t b^{rt} = (ab)^{rt} = e_G$ ist rt durch $\mathrm{ord}(b) = s$ teilbar, und wegen $\mathrm{ggT}(r,s) = 1$ folgt $s \mid t$. Also ist t durch $\mathrm{kgV}(r,s) = rs/\,\mathrm{ggT}(r,s) = rs$ teilbar. Es gilt also $\mathrm{ord}(ab) = t = rs = \mathrm{ord}(a)\,\mathrm{ord}(b)$.
(2) Es sei $r := \mathrm{ord}(a)$, und es sei $d := \mathrm{ggT}(k,r)$. Es gilt $d \mid r$ und $(a^d)^{r/d} = a^r = e_G$, und daher ist r/d durch $\mathrm{ord}(a^d)$ teilbar. Wegen $a^{d\,\mathrm{ord}(a^d)} = e_G$ ist $d\,\mathrm{ord}(a^d)$ durch $\mathrm{ord}(a) = r$ teilbar, und daher gilt: r/d teilt $\mathrm{ord}(a^d)$. Es gilt also $\mathrm{ord}(a^d) = r/d$. Nach (1.9) existieren $x, y \in \mathbb{Z}$ mit $d = kx + ry$. Wegen $a^d = a^{kx+ry} = (a^k)^x(a^r)^y = (a^k)^x \in \langle a^k \rangle$ gilt $\langle a^d \rangle \subset \langle a^k \rangle$, und wegen $a^k = (a^d)^{k/d} \in \langle a^d \rangle$ gilt $\langle a^k \rangle \subset \langle a^d \rangle$. Also gilt $\langle a^k \rangle = \langle a^d \rangle$ und daher

$$\mathrm{ord}(a^k) \;=\; \mathrm{ord}(a^d) \;=\; \frac{r}{d} \;=\; \frac{\mathrm{ord}(a)}{\mathrm{ggT}\big(k, \mathrm{ord}(a)\big)}.$$

(3.8) Definition: Es sei G eine Gruppe. G heißt eine zyklische Gruppe, wenn es ein $a \in G$ mit $G = \langle a \rangle$ gibt. Ist G zyklisch, so heißt jedes $a \in G$ mit $G = \langle a \rangle$ ein erzeugendes Element von G.

(3.9) Bemerkung: (1) Zyklische Gruppen sind abelsch (vgl. (3.2)(2)).
(2) Eine endliche Gruppe G ist genau dann zyklisch, wenn es ein $a \in G$ mit $\mathrm{ord}(a) = \#(G)$ gibt.
(3) Es sei G eine endliche zyklische Gruppe, es sei n die Ordnung von G, und es sei a ein erzeugendes Element von G. Dann gilt $\mathrm{ord}(a) = n$ und $G = \{e_G, a, a^2, \ldots, a^{n-1}\}$ (vgl. (3.5)(1)), und das Rechnen in G erfolgt so: Sind x, $y \in G$, so gibt es eindeutig bestimmte i, $j \in \{0, 1, \ldots, n-1\}$ mit $x = a^i$ und $y = a^j$, und es gilt

$$xy \;=\; a^{i+j} \;=\; a^{(i+j) \bmod n} \quad \text{und} \quad x^{-1} \;=\; a^{-i} \;=\; a^{(-i) \bmod n}.$$

Für $k \in \mathbb{Z}$ gilt nach (3.7)(2): Es ist

$$\operatorname{ord}(a^k) \;=\; \frac{\operatorname{ord}(a)}{\operatorname{ggT}\big(k, \operatorname{ord}(a)\big)} \;=\; \frac{n}{\operatorname{ggT}(k,n)},$$

und daher ist a^k ein erzeugendes Element von G, genau wenn k und n teilerfremd sind. Also ist $\{a^k \mid 0 \le k \le n-1;\ \operatorname{ggT}(k,n) = 1\}$ die Menge aller erzeugenden Elemente von G.

(3.10) Bemerkung: Es sei G eine endliche zyklische Gruppe der Ordnung n, es sei $a \in G$ ein erzeugendes Element von G, und es sei $d \in \mathbb{N}$ ein Teiler von n. Dann gibt es genau eine Untergruppe U_d von G mit $\#(U_d) = d$, und zwar gilt

$$U_d \;=\; \langle\, a^{n/d} \,\rangle \;=\; \{x \in G \mid \operatorname{ord}(x) \text{ teilt } d\} \;=\; \{x \in G \mid x^d = e_G\}.$$

Beweis: Nach (3.7)(2) gilt für die Untergruppe $U_d := \langle\, a^{n/d} \,\rangle$ von G: Es ist

$$\#(U_d) \;=\; \operatorname{ord}(a^{n/d}) \;=\; \frac{\operatorname{ord}(a)}{\operatorname{ggT}\big(n/d, \operatorname{ord}(a)\big)} \;=\; \frac{n}{\operatorname{ggT}(n/d, n)} \;=\; d.$$

Für jedes $x \in U_d$ ist $\operatorname{ord}(x)$ ein Teiler von $\#(U_d) = d$ (vgl. (3.6)(2)), und daher gilt $U_d \subset \{x \in G \mid \operatorname{ord}(x) \text{ teilt } d\} =: U$. Es ist $U = \{x \in G \mid x^d = e_G\}$ (vgl. dazu (3.5)(3)), und für jedes $x \in U$ gilt: Es gibt ein $k \in \mathbb{Z}$ mit $x = a^k$, wegen $a^{kd} = x^d = e_G$ ist kd durch $\operatorname{ord}(a) = n$ teilbar, also k durch n/d, und daher ist $x = a^k \in \langle\, a^{n/d} \,\rangle = U_d$.
Damit ist gezeigt: Es ist $U = U_d$. Ist U' eine Untergruppe von G mit $\#(U') = d$, so gilt $U' \subset \{x \in G \mid \operatorname{ord}(x) \text{ teilt } d\} = U = U_d$ (nach (3.6)(2)) und daher $U' = U_d$.

(3.11) Hilfssatz: *Es sei G eine endliche abelsche Gruppe, und es sei*

$$n \;:=\; \max\big(\{\operatorname{ord}(x) \mid x \in G\}\big).$$

Für jedes $a \in G$ gilt: $\operatorname{ord}(a)$ *teilt n, und es ist $a^n = e_G$.*

Beweis: Es sei $b \in G$ mit $\operatorname{ord}(b) = n$; es sei $a \in G$, und es sei $m := \operatorname{ord}(a)$.
(a) Es sei p eine Primzahl, und es seien $k := v_p(m)$ und $l := v_p(n)$. Dann gilt $m = p^k m_0$ und $n = p^l n_0$ mit natürlichen Zahlen m_0 und n_0, die nicht durch p teilbar sind. Nach (3.7)(2) gilt

$$\operatorname{ord}(a^{m_0}) \;=\; \frac{m}{\operatorname{ggT}(m_0, m)} \;=\; \frac{m}{m_0} \;=\; p^k \quad \text{und}$$

$$\operatorname{ord}(b^{p^l}) \;=\; \frac{n}{\operatorname{ggT}(p^l, n)} \;=\; \frac{n}{p^l} \;=\; n_0.$$

Wegen $p \nmid n_0$ gilt $\mathrm{ggT}(p^k, n_0) = 1$, und daher ist nach (3.7)(1)

$$\mathrm{ord}(a^{m_0} b^{p^l}) \;=\; \mathrm{ord}(a^{m_0}) \cdot \mathrm{ord}(b^{p^l}) \;=\; p^k n_0.$$

Also gilt $p^k n_0 \leq \max(\{\mathrm{ord}(x) \mid x \in G\}) = n = p^l n_0$, und es folgt $k \leq l$.
(b) Nach (a) gilt: Für jede Primzahl p ist $v_p(m) \leq v_p(n)$. Also ist $\mathrm{ord}(a) = m$ ein Teiler von n, und nach (3.5)(3) gilt daher $a^n = e_G$.

(3.12) Bemerkung: Es sei G eine endliche abelsche Gruppe. Die natürliche Zahl

$$\exp(G) \;:=\; \max\big(\{\mathrm{ord}(x) \mid x \in G\}\big)$$

heißt der Exponent der Gruppe G. Der Satz in (3.11) besagt, daß $\exp(G)$ das kleinste gemeinsame Vielfache der Ordnungen der Elemente von G ist.

(3.13) Satz: *Es sei K ein Körper, und es sei G eine endliche Untergruppe der Multiplikativgruppe $K^\times$ von K. Es gilt: Die Gruppe G ist zyklisch.*

Beweis: Es sei $K[T]$ der Polynomring in einer Unbestimmten T über dem Körper K. Mit der im Körper K gegebenen Multiplikation $\cdot$ als Verknüpfung ist $K^\times = K \setminus \{0\}$ eine abelsche Gruppe, deren neutrales Element das Einselement 1_K von K ist. Also ist G eine endliche abelsche Gruppe mit dem neutralen Element 1_K. Es sei $n := \max(\{\mathrm{ord}(x) \mid x \in G\})$ der Exponent von G, und es sei a ein Element von G mit $\mathrm{ord}(a) = n$. Es gilt $n \,|\, \#(G)$ (vgl. (3.6)(2)) und daher $n \leq \#(G)$. Nach (3.11) gilt für jedes $x \in G$: Es ist $x^n = 1_K$, d.h. x ist eine Nullstelle des Polynoms $T^n - 1_K \in K[T]$. Da ein Polynom aus $K[T]$ vom Grad n höchstens n Nullstellen im Körper K besitzt, folgt daraus $\#(G) \leq n$. Also gilt $\#(G) = n = \mathrm{ord}(a) = \#(\langle a \rangle)$, und daher ist $G = \langle a \rangle$.

(3.14) Folgerung: *Ist K ein endlicher Körper, so ist die Multiplikativgruppe $K^\times$ von K eine zyklische Gruppe.*

(3.15) Bemerkung: Es sei G eine abelsche Gruppe, und es sei U eine Untergruppe von G.
(1) Für $a, b \in G$ wird $a \sim b$ gesetzt, genau wenn $a^{-1}b \in U$ ist. Im Beweis von Satz (3.6) wurde gezeigt: $\sim$ ist eine Äquivalenzrelation auf G, und für jedes $a \in G$ ist $[a]_U := aU = \{ax \mid x \in U\}$ die Äquivalenzklasse von a bezüglich $\sim$.
(2) Es seien $a, a', b, b' \in G$, und es gelte $[a]_U = [a']_U$ und $[b]_U = [b']_U$. Dann gilt $a \sim a'$ und $b \sim b'$, also $a^{-1}a' \in U$ und $b^{-1}b' \in U$. G ist abelsch, und U ist eine Untergruppe von G, und daher folgt $(ab)^{-1}(a'b') = (a^{-1}a')(b^{-1}b') \in U$, also $ab \sim a'b'$, also $[ab]_U = [a'b']_U$.
(3) Aus (2) folgt: Man erhält eine wohldefinierte Verknüpfung $\cdot$ auf der Menge

$$G/U \;:=\; \big\{[a]_U \mid a \in G\big\}$$

aller Äquivalenzklassen bezüglich $\sim$ in G, wenn man festsetzt: Für alle $a, b \in G$ sei

$$[a]_U \cdot [b]_U := [ab]_U.$$

(3.16) Satz: *Es sei G eine abelsche Gruppe; es sei U eine Untergruppe von G. Dann ist $G/U = \{[a]_U \mid a \in G\}$ mit der in* (3.15)(3) *erklärten Verknüpfung*

$$([a]_U, [b]_U) \mapsto [ab]_U : G/U \times G/U \to G/U$$

eine abelsche Gruppe; das neutrale Element dieser Gruppe ist $[e_G]_U$, und für jedes $a \in G$ gilt darin: Es ist $[a]_U^{-1} = [a^{-1}]_U$. Ist G endlich, so ist auch G/U endlich, und es gilt $\#(G/U) = \#(G)/\#(U)$.

Beweis: Daß G/U mit der in (3.15)(3) definierten Verknüpfung $\cdot$ eine abelsche Gruppe mit dem neutralen Element $[e_G]_U$ ist und daß darin für jedes $a \in G$ die Äquivalenzklasse $[a^{-1}]_U$ das zu $[a]_U$ inverse Element ist, rechnet man ohne weiteres nach. Daß G/U endlich und $\#(G/U) = \#(G)/\#(U)$ ist, falls G endlich ist, wurde im Beweis von (3.6) gezeigt.

(3.17) Definition: Es sei G eine abelsche Gruppe, und es sei U eine Untergruppe von G. Die abelsche Gruppe G/U mit der Verknüpfung

$$([a]_U, [b]_U) \mapsto [ab]_U : G/U \times G/U \to G/U$$

heißt die Faktorgruppe von G nach U.

(3.18) Bemerkung: Die in diesem Paragraphen zusammengestellten Ergebnisse aus der Theorie der endlichen abelschen Gruppen werden in den folgenden Kapiteln immer wieder verwendet. Näheres dazu und den sonst in diesem Buch benötigten Begriffen aus der Algebra findet man in jedem Lehrbuch der Algebra, zum Beispiel in Artin [7] oder in Scheja-Storch [99].