$P(n) :\iff n$ gerade oder Nachfolger einer geraden Zahl.
Induktionsanfang: $P(0)$ gilt, da 0 gerade.
Induktionsschritt: $P(n)$ möge gelten. Dann gilt $P(n')$:
Beweis: 1. Fall n gerade. Dann ist n' Nachfolger einer geraden Zahl n. Also gilt dann $P(n')$.
2. Fall n ist Nachfolger einer geraden Zahl $2k$, also $n = 2k+1$. Dann ist $n' = n + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$, also gerade. Also gilt dann $P(n')$.
Nach dem Peano-Axiom 5 der vollständigen Induktion gilt $P(n)$ für alle natürlichen Zahlen n.

$$0! = 1$$
$$1! = 0! \cdot 1 = 1 \cdot 1 = 1$$
$$2! = 1! \cdot 2 = 1 \cdot 2 = 2$$
$$3! = 2! \cdot 3 = 2 \cdot 3 = 6$$

Wieviele Möglichkeiten gibt es, 3 Buchstaben a,b,c in einer Reihenfolge anzuordnen?
abc
acb
bac
bca
cab
cba
Insgesamt $3 \cdot 2 \cdot 1 = 3! = 6$ Möglichkeiten.

Wieviele Funktionen $f : \{1, 2, 3\} \to \{x, y\}$ gibt es? Für $f(1)$ gibt es 2 Möglichkeiten x und y. Für $f(2)$ gibt es auch 2 Möglichkeiten, ebenso für $f(3)$. Insgesamt $2 \cdot 2 \cdot 2 = 2^3$ Möglichkeiten.

Wieviele 2-elementige Teilmengen einer 5-elementigen Menge $\{a, b, c, d, e\}$ gibt es?
$\{a, b\}$, $\{a, c\}$, $\{a, d\}$, $\{a, e\}$, $\{b, c\}$, $\{b, d\}$, $\{b, e\}$, $\{c, d\}$, $\{c, e\}$, $\{d, e\}$
$\binom{5}{2} = \frac{5!}{2! \cdot (5-2)!} = \frac{5!}{2! \cdot 3!} = \frac{120}{2 \cdot 6} = 10$ Möglichkeiten.
Wähle Reihenfolge der Elemente, z.B. *dbaec* und wähle davon die ersten 2 Elemente, also im Beispiel: *db*. Dies führt zur Menge $\{b, d\}$. Es gibt 5! mögliche Reihenfolgen. Davon führen jeweils $2! \cdot 3!$ zur gleichen Menge.
$\binom{n}{k}$ ist die Anzahl der k-elementigen Teilmengen einer Menge von n Elementen.

Definition 1 Eine *Halbgruppe* ist ein Paar $(H, *)$ mit

- H ist eine Menge.
- $*$ ist eine assoziative innere Verknüpfung auf H:
  $(a * b) * c = a * (b * c)$ für alle $a, b, c \in H$.

Definition 2 Ein *Monoid* ist ein Paar $(M, *)$ mit

- M ist eine Menge.
- $*$ assoziative innere Verknüpfung auf M mit neutralem Element $e \in M$:
  $(a * b) * c = a * (b * c)$ für alle $a, b, c \in M$.
  $e * a = a * e = a$ für alle $a \in M$.

Beispiel für ein Ideal im Ring $(\mathbb{Z}, +, \cdot)$:
$\{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$ (Menge aller Vielfachen von 3) $= 3\mathbb{Z}$

---

21. Dez 2020

Ideal $(\{2,3\})$:
$\{\dots,-9,-8,-7,-6,-5,-4,-3,-2,-1,0,1,2,3,4,5,6,7,8,9,\dots\}$
Menge $(1) = (\{1\}) = 1\mathbb{Z} = \mathbb{Z}$ aller Vielfachen von 1, also aller ganzen Zahlen.

Ideal $(\{38,8\})$:
$\{\dots,-38,-32,-24,-16,-8,0,$ $\leftarrow$ $\boxed{\text{und alle weiteren negativen Zahlen}}$
$2,4,6,8,10,12,14,16,18,20,22,24,26,28,30,32,34,36,38,\dots\}$
(Menge $(2) = (\{2\})$ aller geraden Zahlen, $(2) = 2\mathbb{Z}$)

Primfaktorzerlegung, z.B. $20 = 2 \cdot 2 \cdot 5$. Beweis der

- Existenz mit Induktion oder Wohlordnung von $\mathbb{N}$.
- Eindeutigkeit mit dem Lemma von Euklid.

11.1.2021

Aufgabe 32

(a) $A = \emptyset \vee |\mathrm{B}| \leq 1 \vee (\mathrm{A,B}\ \text{ endlich })$

(b) $A = \emptyset \vee |\mathrm{B}| \leq 1 \vee (\mathrm{A}\ \text{ endlich } \wedge B \text{ abzählbar})$

18.1.2021

$4 = 2 \cdot 2$ und $6 = 2 \cdot 3$.
$\mathrm{ggT}(4,6) = 2$ und $\mathrm{kgV}(4,6) = 2 \cdot 2 \cdot 3$.

$4 = 2^2 \cdot 3^0$ und $6 = 2^1 \cdot 3^1$.
$\mathrm{ggT}(4,6) = 2^1 \cdot 3^0$ und $\mathrm{kgV}(4,6) = 2^2 \cdot 3^1$.
$\min(2,1) = 1$, $\min(0,1) = 0$
$\max(2,1) = 2$, $\max(0,1) = 1$.

$\min(a,b) + \max(a,b) = a + b$

25.1.2021

Restklassen modulo 3:
Restklasse von 0: $\{\dots,-6,-3,0,3,6,\dots\}$
Restklasse von 1: $\{\dots,-5,-2,1,4,7,\dots\}$
Restklasse von 2: $\{\dots,-4,-1,2,5,8,\dots\}$

Beispiel für eine Untergruppe von $(\mathbb{Z},+)$:
$(\{\dots,-6,-3,0,3,6,\dots\},+)$.
Wir schreiben für $\{\dots,-6,-3,0,3,6,\dots\}$ auch $3\mathbb{Z}=\{3n \mid n\in\mathbb{Z}\}$.

$(U,*)$ ist eine Untergruppe von $(G,*)$ genau dann, wenn $U\subseteq G$ und

- $e\in U$
- Wenn $a,b\in U$, dann $a*b\in U$.
- Wenn $a\in U$, dann $a^{-1}\in U$.

Die von A erzeugte Untergruppe von $(G,*)$ ist die Menge aller Elemente von G, die sich ergeben als e oder aus Elementen von A durch $*$ und $\cdot^{-1}$.

Beispiel: Die von $\{3\}$ erzeugte Untergruppe von $(\mathbb{Z},+)$ ist $\{\dots,-6,-3,0,3,6,\dots\}$, also $3\mathbb{Z}$.

Beispiel: Gruppe $(\mathbb{Q}\setminus\{0\},\cdot)$. Die von der Zahl 3 erzeugte Untergruppe ist $\{\dots,\frac{1}{27},\frac{1}{9},\frac{1}{3},1,3,9,27,\dots\}=\{3^n\mid n\in\mathbb{Z}\}$.
Allgemein in einer Gruppe $(G,*)$ mit neutralem Element e: $a^0=e$, $a^1=a$, $a^2=a*a$, $a^3=a*a*a$, ... und a^{-1} Inverses von a, $a^{-2}=a^{-1}*a^{-1}$, $a^{-3}=a^{-1}*a^{-1}*a^{-1}$, ...
Die von a erzeugte Untergruppe ist $\{a^n\mid n\in\mathbb{Z}\}$.

Sei $(G,*)$ eine endliche Gruppe. Dann sind nicht alle a^n mit $n>0$ voneinander verschieden. Z.B. $a*a=a*a*a*a*a$. Dann gilt $e=a*a*a^{-1}*a^{-1}=a*a*a*a*a*a^{-1}*a^{-1}=a*a*a$.

Dann gibt es ein $n \in \mathbb{Z}$ mit $a^n = e$. Die Ordnung von a ist die kleinste solche Zahl n, also die Ordnung der von a erzeugten Untergruppe $\{a^n \mid n \in \mathbb{Z}\}$.

Gruppe $(\mathbb{Z}/4\mathbb{Z}, +)$ der Restklassen modulo 4 mit der Addition. Die von $[2]_{\equiv_4}$ (hier kurz $[2]$ oder $\overline{2}$) erzeugte Untergruppe ist $\{[0], [2]\}$ und hat Ordnung 2. Also hat $[2]$ die Ordnung 2. Kleinste positive ganze Zahl n mit $[2] \cdot n = [0]$ ist 2.

$(3\mathbb{Z}, +)$ ist Untergruppe von $(\mathbb{Z}, +)$. Nebenklassen dieser Untergruppe sind die Restklassen modulo 3:
$0 + 3\mathbb{Z}$, $1 + 3\mathbb{Z}$ und $2 + 3\mathbb{Z}$.

Die Nebenklassen von U bilden eine Partition von G.

In einer Gruppe $(G, *)$ gibt es zu allen $a, b \in G$ ein und nur ein x mit $a * x = b$. Es ist $x = a^{-1} * b$.
In einer Gruppe $(G, *)$ gibt es zu allen $a, b \in G$ ein und nur ein x mit $x * a = b$. Es ist $x = b * a^{-1}$.
In der Gruppentafel kommt in jeder Zeile jedes Gruppenelement genau einmal vor; genauso in jeder Spalte.

Aufgabe 63: alle $n\mathbb{Z}$.
Aufgabe 64: $H = 3\mathbb{Z}$. Nebenklassen: $3\mathbb{Z}$, $1 + 3\mathbb{Z}$ und $2 + 3\mathbb{Z}$, also alle Restklassen modulo 3.

Restklassenring modulo 6 ist kein Körper, weil 6 keine Primzahl ist, sondern $6 = 2 \cdot 3$ und daher $[2] \cdot [3] = [0]$, also $[2]$ und $[3]$ Nullteiler sind. Einheitengruppe ist $(\{[1], [5]\}, \cdot)$.